KASPERSKY LAB

Kaspersky® Anti-Virus for Windows Servers 6.0

USER GUIDE

KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

User Guide

© Kaspersky Lab
http://www.kaspersky.com

Revision date: July 2007

Table of Contents

CHAPTER 1. THREATS TO COMPUTER SECURITY 9
1.1. Sources of Threats 9
1.2. How threats spread 10
1.3. Types of Threats 11

CHAPTER 2. KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0 14
2.1. What's new in Kaspersky Anti-Virus for Windows Servers 6.0 14
2.2. The elements of Kaspersky Anti-Virus for Windows Servers Defense 15
2.2.1. File Anti-Virus 16
2.2.2. Virus scan tasks 16
2.2.3. Program tools 17
2.3. Hardware and software system requirements 18
2.4. Software packages 19
2.5. Support for registered users 19

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0 21
3.1. Installation procedure using the Installation Wizard 22
3.2. Setup Wizard 26
3.2.1. Using objects saved with Version 5.0 26
3.2.2. Activating the program 26
3.2.2.1. Selecting a program activation method 27
3.2.2.2. Entering the activation code 27
3.2.2.3. Obtaining a key file 28
3.2.2.4. Selecting a license key file 28
3.2.2.5. Completing program activation 28
3.2.3. Configuring update settings 29
3.2.4. Configuring a virus scan schedule 29
3.2.5. Restricting program access 30
3.2.6. Finishing the Setup Wizard 30
3.3. Installing the program from the command prompt 31
3.4. Procedure for installing the Group Policy Object 32

3.4.1. Installing the program 32
3.4.2. Upgrading the program 33
3.4.3. Uninstalling the program 33
3.5. Upgrading from 5.0 to 6.0 33

CHAPTER 4. PROGRAM INTERFACE 35
4.1. System tray icon 35
4.2. The context menu 36
4.3. Main program window 37
4.4. Program settings window 39

CHAPTER 5. GETTING STARTED 41
5.1. What is the protection status of my computer? 41
5.1.1. Protection indicators 41
5.1.2. Kaspersky Anti-Virus for Windows Servers component status 44
5.1.3. Program performance statistics 46
5.2. How to scan your server for viruses 46
5.3. How to scan critical areas of the computer 47
5.4. How to scan a file, folder or disk for viruses 47
5.5. How to update the program 48
5.6. What to do if protection is not running 49

CHAPTER 6. PROTECTION MANAGEMENT SYSTEM 50
6.1. Stopping and resuming protection on your computer 50
6.1.1. Pausing protection 51
6.1.2. Stopping server protection 52
6.1.3. Pausing / stopping protection 52
6.1.4. Restoring protection on your computer 53
6.1.5. Shutting down the program 54
6.2. Types of malicious programs to be monitored 54
6.3. Creating a trusted zone 55
6.3.1. Exclusion rules 56
6.3.2. Trusted applications 59
6.4. Starting tasks under another profile 61
6.5. Configuring Scheduled Tasks and Notifications 62
6.6. Power options 64
6.7. Multi-processor server configuration 65

CHAPTER 7. ANTI-VIRUS PROTECTION OF THE SERVER FILE SYSTEM 66
7.1. Selecting a file security level 67
7.2. Configuring File Anti-Virus 68
7.2.1. Defining the file types to be scanned 69
7.2.2. Defining protection scope 71
7.2.3. Configuring advanced settings 73
7.2.4. Restoring default File Anti-Virus settings 75
7.2.5. Selecting actions for objects 75
7.2.6. Creating a notification template 77
7.3. Postponed disinfection 77

CHAPTER 8. SCANNING FOR VIRUSES ON YOUR COMPUTER 79
8.1. Managing virus scan tasks 80
8.2. Creating a list of objects to scan 80
8.3. Creating virus scan tasks 81
8.4. Configuring virus scan tasks 82
8.4.1. Selecting a security level 83
8.4.2. Specifying the types of objects to scan 84
8.4.3. Restoring default scan settings 87
8.4.4. Selecting actions for objects 87
8.4.5. Additional virus scan settings 89
8.4.6. Setting up global scan settings for all tasks 90

CHAPTER 9. TESTING KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS 92
9.1. The EICAR test virus and its variations 92
9.2. Testing File Anti-Virus 94
9.3. Testing virus scan tasks 95

CHAPTER 10. PROGRAM UPDATES 96
10.1. Starting the Updater 97
10.2. Rolling back to the previous update 98
10.3. Creating update tasks 98
10.4. Configuring update settings 99
10.4.1. Selecting an update source 100
10.4.2. Selecting an update method and what to update 102
10.4.3. Configuring connection settings 104
10.4.4. Update distribution 105

10.4.5. Actions after updating the program ... 106

CHAPTER 11. ADVANCED OPTIONS ... 108
11.1. Quarantine for potentially infected objects ... 109
11.1.1. Actions with quarantined objects ... 110
11.1.2. Setting up Quarantine ... 111
11.2. Backup copies of dangerous objects ... 112
11.2.1. Actions with backup copies ... 113
11.2.2. Configuring Backup settings ... 114
11.3. Reports ... 114
11.3.1. Configuring report settings ... 117
11.3.2. The *Detected* tab ... 117
11.3.3. The *Events* tab ... 118
11.3.4. The Statistics tab ... 119
11.3.5. The Settings tab ... 120
11.3.6. The *Banned users* tab ... 121
11.4. General information about the program ... 122
11.5. Managing licenses ... 123
11.6. Technical Support ... 124
11.7. Configuring the Kaspersky Anti-Virus for Windows Servers interface ... 126
11.8. Using advanced options ... 128
11.8.1. Kaspersky Anti-Virus for Windows Servers event notifications ... 128
11.8.1.1. Types of events and notification delivery methods ... 129
11.8.1.2. Configuring email notification ... 131
11.8.1.3. Configuring event log settings ... 132
11.8.2. Self-Defense and access restriction ... 133
11.8.3. Resolving conflicts with other applications ... 134
11.9. Importing and exporting Kaspersky Anti-Virus for Windows Servers settings ... 135
11.10. Resetting to default settings ... 135

CHAPTER 12. ADMINISTERING THE PROGRAM WITH KASPERSKY ADMINISTRATION KIT ... 137
12.1. Administering the application ... 139
12.1.1. Starting/stopping the application ... 140
12.1.2. Configuring application settings ... 141
12.1.3. Configuring specific settings ... 142

12.2. Managing tasks 143
12.2.1. Starting and stopping tasks 144
12.2.2. Creating tasks 145
12.2.2.1. Creating local tasks 145
12.2.2.2. Creating group tasks 147
12.2.2.3. Creating global tasks 147
12.2.3. Configuring task settings 148
12.3. Managing policies 149
12.3.1. Creating policies 149
12.3.2. Viewing and editing policy settings 151

CHAPTER 13. WORKING WITH THE PROGRAM FROM THE COMMAND PROMPT 153
13.1. Activating the application 154
13.2. Managing File Anti-Virus and tasks 155
13.3. Anti-virus scans 158
13.4. Program updates 161
13.5. Rollback settings 163
13.6. Exporting settings 163
13.7. Importing settings 164
13.8. Starting the program 165
13.9. Stopping the program 165
13.10. Obtaining a Trace File 165
13.11. Viewing Help 166
13.12. Return codes from the command line interface 166

CHAPTER 14. MODIFYING, REPAIRING, AND REMOVING THE PROGRAM 168
14.1. Modifying, repairing, and removing the program using Installation Wizard 168
14.2. Uninstalling the program from the command prompt 170

APPENDIX A. REFERENCE INFORMATION 172
A.1. List of files scanned by extension 172
A.2. Possible file exclusion masks 174
A.3. Possible Virus Encyclopedia classification exclusion masks 175
A.4. Overview of settings in *setup.ini* 176

APPENDIX B. KASPERSKY LAB 177
B.1. Other Kaspersky Lab Products 178

B.2. Contact Us..... 188

APPENDIX C. LICENSE AGREEMENT 190

CHAPTER 1. THREATS TO COMPUTER SECURITY

As information technology has rapidly developed and penetrated many aspects of human existence, so the number and range of crimes aimed at breaching information security has grown.

Cyber criminals have shown great interest in the activities of both state structures and commercial enterprises. They attempt to steal or disclose confidential information, which damages business reputations, disrupts business continuity, and may impair an organization's information resources. These acts can do extensive damage to assets, both tangible and intangible.

It is not big companies alone who are at risk. Individual users can also be attacked. Using various tools, criminals gain access to personal data (bank account and credit card numbers and passwords), cause your system to malfunction, or gain complete access to your computer. Then that computer can be used as part of a zombie network, a network of infected computers used by hackers to attack servers, send out spam, harvest confidential information, and spread new viruses and Trojans.

In today's world, it is widely acknowledged that information is a valuable asset that should be protected. At the same time, information must be accessible to those who legitimately require it (for instance, employees, clients and partners of a business). Hence, the need to create a comprehensive information security system, which must take account of all possible sources of threats, whether human, man-made, or natural disasters, and use a complete array of defensive measures, at the physical, administrative and software levels.

1.1. Sources of Threats

A person, a group of people, or phenomena unrelated to human activity can threaten information security. Following from this, all threat sources can be put into one of three groups:

- **The human factor**. This group of threats concerns the actions of people with authorized or unauthorized access to information. Threats in this group can be divided into:
    - *External*, including cyber criminals, hackers, internet scams, unprincipled partners, and criminal organizations.

- *Internal*, including the actions of company staff. Actions taken by this group could be deliberate or accidental.

- **The technological factor**. This threat group is connected with technical problems – use of obsolete or poor-quality software and hardware to process information. This can lead to equipment failure and often to data loss.

- **The natural-disaster factor**. This threat group includes the whole range of events caused by nature and independent of human activity.

All three threat sources must be accounted for when developing a data security protection system. This User Guide focuses on the area that is directly tied to Kaspersky Lab's expertise – external threats involving human activity.

1.2. How threats spread

As modern computer technology and communications tools develop, hackers have more opportunities for spreading threats. Let's take a closer look at them:

The Internet

The Internet is unique, since it is no one's property and has no geographical borders. In many ways, this has promoted the development of web resources and the exchange of information. Today, anyone can access data on the Internet or create their own webpage.

However, these very features of the worldwide web give hackers the ability to commit crimes on the Internet, and make the hackers difficult to detect and punish.

Hackers place viruses and other malicious programs on Internet sites and disguise them as useful freeware. Furthermore, scripts that run automatically when you open certain web pages can execute dangerous actions on your computer, including modifying the system registry, stealing personal data, and installing malicious software.

By using network technologies, hackers can attack company servers. These attacks can cause parts of your system to malfunction, or could provide hackers with complete access to your system and thereby to the information stored on it. They can also use it as part of a zombie network.

Intranet

Your intranet is your internal network, specially designed for handling information within a company or a home network. An intranet is a unified space for storing, exchanging, and accessing information for all the computers on the network. This means that if one computer on the network is infected, the others are at great risk of infection. To avoid such

situations, both the network perimeter and each individual computer must be protected.

Email

Since the overwhelming majority of computers have email client programs installed, and since malicious programs exploit the contents of electronic address books, conditions are usually right for spreading malicious programs. The user of an infected computer might, without realizing, send infected emails to friends or coworkers who in turn send more infected emails. For example, it is common for infected file documents to go undetected when distributed with business information via a company's internal email system. When this occurs, more than a handful of people are infected. It might be hundreds or thousands of company workers, together with potentially tens of thousands of subscribers.

Removable storage media

Removable media (floppies, CD/DVD-ROMs, and USB flash drives) are widely used for storing and transmitting information.

Opening a file that contains malicious code and is stored on a removable storage device can damage data stored on the local computer and spread the virus to the computer's other drives or other computers on the network.

1.3. Types of Threats

There are a vast number of threats to computer security today. This section will review the threats that are blocked by Kaspersky Anti-Virus for Windows Servers.

Worms

This category of malicious programs spreads itself largely by exploiting vulnerabilities in computer operating systems. The class was named for the way that worms crawl from computer to computer, using networks and email. This feature allows worms to spread themselves very rapidly.

Worms penetrate a computer, search for the network addresses of other computers, and send a burst of self-made copies to these addresses. In addition, worms often utilize data from email client address books. Some of these malicious programs occasionally create working files on system disks, but they can run without any system resources except RAM.

Viruses

Viruses are programs that infect other files, adding their own code to them to gain control of the infected files when they are opened. This simple

definition explains the fundamental action performed by a virus – *infection*.

Trojans

Trojans are programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang, stealing confidential information, and so on. This class of malicious program is not a virus in the traditional sense of the word, because it does not infect other computers or data. Trojans cannot break into computers on their own and are spread by hackers, who disguise them as regular software. The damage that they inflict can greatly exceed that done by traditional virus attacks.

Recently, worms have been the commonest type of malicious program damaging computer data, followed by viruses and Trojans. Some malicious programs combine features of two or even three of these classes.

Adware

Adware comprises programs that are included in software, unknown to the user, which is designed to display advertisements. Adware is usually built into software that is distributed free. The advertisement is situated in the program interface. These programs also frequently collect personal data on the user and send it back to their developer, change browser settings (start page and search pages, security levels, etc.) and create traffic that the user cannot control. This can lead to a security breach and to direct financial losses.

Spyware

This software collects information about a particular user or organization without their knowledge. Spyware often escapes detection entirely. In general, the goal of spyware is to:

- trace user actions on a computer
- gather information on the contents of your hard drive; in such cases, this usually involves scanning several directories and the system registry to compile a list of software installed on the computer
- gather information on the quality of the connection, bandwidth, modem speed, etc.

Riskware

Riskware is potentially dangerous software that does not have a malicious function but, since it contains holes and errors, can be used by hackers as an auxiliary component for a malicious program. Under certain conditions, having such programs on a computer can put data at risk.

These programs include, for instance, some remote administration utilities, keyboard layout togglers, IRC clients, FTP servers, and all-purpose utilities for stopping or hiding processes.

Another type of malicious program that is similar to adware, spyware, and riskware are programs that plug into your web browser and redirect traffic.

Jokes

Joke software does not do any direct damage, but displays messages stating that damage has already been done or will be under certain conditions. These programs often warn the user of non-existent dangers, such as messages that warn of formatting the hard drive (although no formatting actually takes place) or detecting viruses in uninfected files.

Rootkits

These are utilities that are used to conceal malicious activity. They mask malicious programs to keep anti-virus programs from detecting them. Rootkits modify basic functions of the computer's operating system to hide both their own existence and actions that the hacker undertakes on the infected computer.

Other dangerous programs

These are programs created to, for instance, set up denial of service (DoS) attacks on remote servers, hack into other computers, and programs that are part of the development environment for malicious programs. These programs include hack tools, virus builders, vulnerability scanners, password-cracking programs, and other types of programs for cracking network resources or penetrating a system.

Warning!

From this point forward, we will use the term "virus" to refer to malicious and dangerous programs. There will only be emphasis placed on the type of malicious programs where necessary.

CHAPTER 2. KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Kaspersky Anti-Virus for Windows Servers 6.0 heralds a new generation of data security products.

2.1. What's new in Kaspersky Anti-Virus for Windows Servers 6.0

Let's take a closer look at the new features in Kaspersky Anti-Virus for Windows Servers.

New Protection Features

- The program's file protection technology has been changed: now you can lower the load on the central processor and disk subsystems and increase the speed of file scans. iChecker and iSwift make this possible. By operating this way, the application will not scan files twice.
- The scan process now runs as a background task, enabling the administrator to continue using the computer. If there is a competition for system resources, the virus scan will pause until the user's operation is completed and then resumes at the point where it left off.
- Critical areas of the server where infection could lead to serious consequences are given their own separate task. You can configure this task to run automatically every time the system is started.
- The user notification function (see 11.8.1 on pg. 128) has been expanded for certain events that arise during program operation. You can select the method of notification yourselves for each of these event types: e-mails, sound notifications, pop-up messages.
- New features included application self-defense technology, protection from unauthorized remote access of program services, protection of application files from unauthorized access or modification, and password protection for program settings.

New Program Interface Features

- The new Kaspersky Anti-Virus for Windows Servers interface makes the program's functions clear and easy to use. You can also change the program's appearance by using your own graphics and color schemes.
- The program regularly provides you with tips as you use it: Kaspersky Anti-Virus for Windows Servers displays informative messages on the level of protection, accompanies its operation with hints and tips, and includes a thorough Help section.

New Program Update Features

- This version of the application debuts our improved update procedure: Kaspersky Anti-Virus automatically checks the update source for update packages. When Anti-Virus detects fresh updates, it downloads them and installs them on the computer.
- The program downloads updates incrementally, ignoring files that have already been downloaded. This lowers the download traffic for updates by up to 10 times.
- Updates are downloaded from the most efficient source.
- The program has an update rollback feature that can return to the previous version of the signatures, if, for example, the threat signatures are damaged or there is an error in copying.
- A feature has been added for distributing updates to a local folder to give other network computers access to them to save bandwidth.

2.2. The elements of Kaspersky Anti-Virus for Windows Servers Defense

Kaspersky Anti-Virus for Windows Servers protection includes:

- File Anti-Virus (see 2.2.1 on pg. 16), which monitors the computer's file system in real-time mode.
- Virus Scan Tasks (see 2.2.2 on pg. 16) that virus-check the computer's memory and file system, as individual files, folders, disks, or regions.
- Support Tools (see 2.2.3 on pg. 17) that provide support for the program and extend its functionality.

2.2.1. File Anti-Virus

The server is protected in real-time using **File Anti-Virus**.

A file system can contain viruses and other dangerous programs. Malicious programs can be stored in a file system for years after one day making it through on a floppy disk or from the Internet, without showing themselves at all. But you need only open the infected file, and the virus is instantly activated.

File Antivirus is the component that monitors your computer's file system. It scans all files that are being opened, executed or saved on the server and all connected disk drives. Kaspersky Anti-Virus intercepts every attempt to access a file and scans the file for known viruses. The file can only be used further if the file is not infected or is successfully treated by File Anti-Virus. If a file cannot be disinfected for any reason, it will be deleted, with a copy of the file saved in Backup (see 11.2 on pg. 112), or moved to Quarantine (see 11.1 on pg. 109).

2.2.2. Virus scan tasks

In addition to constantly monitoring all potential pathways for malicious programs using File Anti-Virus, it is extremely important to periodically scan your computer for viruses. This is necessary to detect malicious programs that were not previously discovered by File Anti-Virus because, for instance, its security level was set too low.

Kaspersky Anti-Virus for Windows Servers configures, by default, the following virus-scan tasks:

Critical Areas

Scans all critical areas of the computer for viruses. This includes system memory, programs loaded on startup, boot sectors on the hard drive, and the *Microsoft Windows* system directories. The task aims to detect active viruses quickly without fully scanning the computer.

My Computer

Scans for viruses on your computer with a through inspection of all disk drives, memory, and files.

Startup Objects

Scans for viruses in all programs that are loaded automatically on startup, plus RAM and boot sectors on hard drives.

There is also the option to create other virus-scan tasks and create a schedule for them.

2.2.3. Program tools

Kaspersky Anti-Virus for Windows Servers includes a number of support tools, which are designed to provide real-time software support, expanding the capabilities of the program and assisting you as you go.

Update

In order to be prepared to delete a virus or some other dangerous program, Kaspersky Anti-Virus for Windows Servers needs to be kept up-to-date. The *Update* component is designed to do exactly that. It is responsible for updating the Kaspersky Anti-Virus for Windows Servers threat signatures and program modules.

The Update Distribution feature enables you to save updates for the threat signature database and application modules retrieved from Kaspersky Lab update servers and then give other computers access to them to save bandwidth.

Data Files

File Anti-Virus and each virus scan and program update create a report as they run. The reports contain information on completed operations and their results. By using the *Reports* feature, you will remain up-to-date on the operation of any Kaspersky Anti-Virus for Windows Servers components. Should problems arise, the reports can be sent to Kaspersky Lab, allowing our specialists to study the situation in greater depth and help you as quickly as possible.

Kaspersky Anti-Virus for Windows Servers sends all files suspected of being dangerous to a special *Quarantine* area, where they are stored in encrypted form to avoid infecting the computer. You can scan these objects for viruses, restore them to their previous locations, delete them, or manually add files to Quarantine. Files that turn out uninfected upon completion of the virus scan are automatically restored to their former locations.

The *Backup* area holds copies of files disinfected and deleted by the program. These copies are created in case you need either to restore the files, or want information about their infection. These backup copies are also stored in an encrypted form to avoid further infection.

You can manually restore a file from Backup to the original location and delete the copy.

Support

All registered Kaspersky Anti-Virus users can take advantage of our technical support service. To learn where exactly you can get technical support, use the *Support* feature.

Using the links, you can go to the Kaspersky Lab users forum and browse frequently asked questions with answers that might help you solve your problem. You can also send an error report or question on program operation to Technical Support by completing an on-line form.

You will also be able to access Technical Support on-line, and, of course, our employees will always be ready to assist you with Kaspersky Anti-Virus by phone.

2.3. Hardware and software system requirements

For Kaspersky Anti-Virus to run properly, your computer must meet these minimum requirements:

General Requirements:

- 50 MB available space on your hard drive
- CD-ROM (for installing Kaspersky Anti-Virus for Windows Servers 6.0 from the installation CD)
- Microsoft Internet Explorer 5.5 or higher (for updating threat signatures and program modules through the Internet)
- Microsoft Windows Installer 2.0

Operating system:

- Microsoft Windows 2000 Server/Advanced Server Service Pack 4 or higher, all available updates.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, all Service Packs, all available updates.
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Software packages

You can purchase the boxed version of Kaspersky Anti-Virus for Windows Servers from our resellers, or download it from Internet shops, including the **eStore** section of www.kaspersky.com.

If you buy the boxed version of the program, the package will include:

- A sealed envelope with an installation CD containing the program files
- A license key, included with the installation package or on a special diskette, or an application activation code on the CD slip.
- A User Guide
- The end-user license agreement (EULA)

Before breaking the seal on the installation disk envelope, carefully read through the EULA.

If you buy Kaspersky Anti-Virus for Windows Servers from an online store, you copy the product from the Kaspersky Lab website (**Downloads → Product Downloads**). You can download the User Guide from the **Downloads → Documentation** section.

You will be sent a license key or activation code by email after your payment has been received.

The End-User License Agreement is a legal agreement between you and Kaspersky Lab that specifies the terms on which you may use the software you have purchased.

Read the EULA through carefully.

If you do not agree with the terms of the EULA, you can return your boxed product to the reseller from whom you purchased it and be reimbursed for the amount you paid for the program. If you do so, the sealed envelope for the installation disk must still be sealed.

By opening the sealed installation disk, you accept all the terms of the EULA.

2.5. Support for registered users

Kaspersky Lab provides its registered users with an array of services to make Kaspersky Anti-Virus for Windows Servers more effective.

When the program has been activated, you become a registered user and will have the following services available until the license expires:

- New versions of the program free of charge
- Consultation on questions regarding installation, configuration, and operation of the program, by phone and email
- Notifications on new Kaspersky Lab product releases and new viruses (this services is for users that subscribe to Kaspersky Lab news mailings)

Kaspersky Lab does not provide technical support for operating system use and operation, or for any products other than its own.

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

There are several ways to install Kaspersky Anti-Virus 6.0 for Windows Servers:

- Local Installation: install the application on a single host. Direct access to the host in question is required to run and complete the install. A local install may be performed in one of the two modes below:
    - an interactive install using the application Installation Wizard (see 3.1 on pg. 22); this mode requires user input for the install to proceed;
    - a non-interactive install run from the command line using default settings and not requiring any user input for the install to proceed (see 3.3 on pg. 31).
- Remote Installation: install the application to networked computers remotely from an administrator workstation using:
    - the Kaspersky Administration Kit software suite (cf. Kaspersky Administration Kit Implementation Guide);
    - Microsoft Windows Server 2000/2003 group domain policies (see 3.4 on pg. 32).

It is recommended that all running applications be closed prior to Kaspersky Anti-Virus installation (including a remote installation).

In the event that you already have Kaspersky Anti-Virus 5.0 installed, it will be removed and updated to Kaspersky Anti-Virus 6.0 when the installation procedure is run (see 3.5 on pg. 33 for more detail). Updates to more recent builds (minor versions) within Kaspersky Anti-Virus 6.0 are transparent.

3.1. Installation procedure using the Installation Wizard

To install Kaspersky Anti-Virus for Windows Servers on your computer, open the Windows Installer file on the installation CD.

> Note:
>
> Installing the program with an installer package downloaded from the Internet is identical to installing it from an installation CD.

An installation wizard will open for the program. Each window contains a set of buttons for navigating through the installation process. Here is a brief explanation of their functions:

- **Next** – accepts an action and moves forward to the next step of installation.
- **Back** – goes back to the previous step of installation.
- **Cancel** – cancels product installation.
- **Finish** – completes the program installation procedure.

Let's take a closer look at the steps of the installation procedure.

Step 1. Checking for the necessary system conditions to install Kaspersky Anti-Virus for Windows Servers

Before the program is installed on your computer, the installer checks your computer for the operating system and service packs necessary to install Kaspersky Anti-Virus for Windows Servers. It also checks your computer for other necessary programs and verifies that your user rights allow you to install software.

If any of these requirements is not met, the program will display a message informing you of the fault. You are advised to install any necessary service packs through **Windows Update**, and any other necessary programs, before installing Kaspersky Anti-Virus for Windows Servers.

Step 2. Installation Welcome window

If your system fully meets all requirements, an installation window will appear when you open the installer file with information on beginning the installation of Kaspersky Anti-Virus for Windows Servers.

To continue installation, click the **Next** button. You may cancel installation by clicking **Cancel**.

Step 3. Viewing the End-User License Agreement

The next window contains the End-User License Agreement which is made between you and Kaspersky Lab. Carefully read through it, and if you agree to all the terms of the agreement, select **I accept the terms of the License Agreement** and click the **Next** button. Installation will continue.

To cancel installation click **Cancel**.

Step 4. Selecting an installation folder

The next stage of Kaspersky Anti-Virus for Windows Servers installation determines where the program will be installed on your computer. The default path is:

- **<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers** – for 32-bit systems
- **<Drive>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers** – for 64-bit systems

You can specify a different folder by clicking the **Browse** button and selecting it in the folder selection window, or by entering the path to the folder in the field available.

Remember that if you enter the full path to the installation folder manually, its length must not exceed 200 characters or contain special characters.

To continue installation, click the **Next** button.

Step 5. Using Saved Installation Settings

In this step, you are prompted to specify whether you wish to use previously saved security settings or threat signatures if these were in fact saved when a previous Kaspersky Anti-Virus 6.0 installation was removed from your server.

Let's take a closer look at how to use the options described above.

If you have previously installed another version or build of Kaspersky Anti-Virus for Windows Servers on your computer and you saved its threat signatures when you uninstalled it, you can use it in the current version. To do so, check **Threat signatures**. The threat signatures included with the program installation will not be copied to the server.

To use protection settings that you configured and saved from a previous version, check **Protection settings**.

Step 6. Selecting an installation type

In this stage, you select how much of the program you want to install on your computer. You have three options:

Complete. If you select this option, all Kaspersky Anti-Virus for Windows Servers components will be installed.

Custom. If you select this option, you can select the program components that you want to install. For more, see Step 7.

To select a setup type, click the appropriate button.

Step 7. Selecting program components to install

This step occurs only if you select the **Custom** setup type.

If you selected Custom installation, you can select the components of Kaspersky Anti-Virus for Windows Servers that you want to install. By default, File Anti-Virus, the virus scan component, and connector to the Administration Agent for remote administration via Kaspersky Administration Kit are selected for installation.

To select the components you want to install, left-click the icon alongside a component name and select **Will be installed on local hard drive** from the opened menu. You will find more information on what protection a selected component provides, and how much disk space it requires for installation, in the lower part of the program installation window.

If you do not want to install a component, select **Entire feature will be installed on local hard drive** item from the context menu.

After you have selected the components you want to install, click **Next**. To return the list to the default programs to be installed, click **Reset**.

Step 8. Searching for other anti-virus programs

In this stage, the installer searches for other anti-virus products installed on the server, including Kaspersky Lab products, which could raise compatibility issues with Kaspersky Anti-Virus for Windows Servers.

The installer will display on screen a list of any such programs it detects. The program will ask you if you want to uninstall them before continuing installation.

You can select manual or automatic uninstall under the list of anti-virus applications detected (only Kaspersky Lab products will be deleted automatically).

To continue installation, click the **Next** button.

Step 9. Finishing installing your program

In this stage, the program will ask you to finish installing the program on the server.

We do not recommend deselecting the **Enable Self-Defense before installation** when initially installing Kaspersky Anti-Virus 6.0. By enabling the protection modules, you can correctly roll back installation if errors occur while installing the program. If you are reinstalling the program, we recommend that you deselect this checkbox.

If the application is installed remotely via **Windows Remote Desktop**, we recommend checking **Enable Self-Defense before installation**. Otherwise the installation procedure might not finish or finish correctly.

If you want exclusions recommended by Microsoft for servers to be added to the exclusions automatically, check **Exclude areas recommended by Microsoft from virus scan**.

If you want the environment variable %Path% to be added to avp.com after installation, check **Add path to avp.com to system variable %PATH%**.

To continue installation, click the **Next** button.

Warning!

When Kaspersky Anti-Virus components which intercept network traffic are being installed current network connections are broken. Most of them will be recovered in some period of time.

Step 10.Completing the installation procedure

The **Complete Installation** window contains information on finishing the Kaspersky Anti-Virus installation process.

To start the setup wizard, click the **Next** button (see 3.2 on pg. 26).

If installation is completed successfully, you will need to restart your computer, and a message on the screen will tell you so.

3.2. Setup Wizard

The Kaspersky Anti-Virus for Windows Servers 6.0 Setup Wizard starts after the program has finished installation. It is designed to help you configure the initial program settings to conform to the features and uses of your computer.

The Setup Wizard interface is designed as a standard Windows Wizard and consists of a series of steps that can be navigated using the **Back** and **Next** buttons, or complete using the **Finish** button. The **Cancel** button will stop the Wizard at any point.

If you stop the setup wizard by closing the wizard window, the application will not run. Every time you start the application, the setup wizard will start over until the setup procedure is completed successfully.

3.2.1. Using objects saved with Version 5.0

This wizard window appears after finishing the application installation process on top of Kaspersky Anti-Virus 5.0. You will be asked to select what data used by version 5.0 you want to import to version 6.0. This might include quarantined or backup files or protection settings.

To use this data in Version 6.0, check the necessary boxes.

3.2.2. Activating the program

Before activating the program, make sure that the computer's system date settings match the actual date and time.

The program is activated by installing a license key that Kaspersky Anti-Virus will use to check for a license and to determine the expiration date for it.

The license key contains system information necessary for all the program’s features to operate, and other information:

- Support information (who provides program support and where you can obtain it)
- Name, number, and expiration date of your license

3.2.2.1. Selecting a program activation method

Depending on whether you have a key for Kaspersky Anti-Virus or need to obtain one from the Kaspersky Lab server, you have several options for activating the program:

- **Activate using the activation code**. Select this activation option if you have purchased the full version of the program and were provided with an activation code. Using this activation code you will obtain a key file providing access to the application's full functionality throughout the effective term of the license agreement.

- **Activate trial version.** Select this activation option if you want to install the trail version of the program before making the decision to buy a commercial version. You will be given a free key valid for a term specified in the trial version license agreement.

- **Apply existing license key**. Activate the application using a Kaspersky Anti-Virus 6.0 license key file.

- **Activate later**. If you choose this option, you will skip the activation stage. Kaspersky Anti-Virus for Windows Servers 6.0 will be installed on your computer and you will have access to all program features except updates (you can only update the threat signatures once after installing the program).

The first two activation options use a Kaspersky Lab web server, which requires an Internet connection. Before activating, make sure to edit your network settings (see 10.4.3 on p. 104) in the window that opens when you click **LAN settings** (if necessary). For more in-depth information on configuring network settings, contact your system administrator or ISP.

If you have no Internet connection when installing the program you can activate the application later (see 11.5 on pg. 123) using its interface or you can use Internet access of another computer to register at Kaspersky Lab Technical Support website and get the key using activation code

3.2.2.2. Entering the activation code

You must enter an activation code to activate the program. If you purchase the program through the Internet, you will receive the activation code by e-mail. If you purchase a boxed version of the program, you will find the activation code on the installation CD-ROM envelope.

The activation code is a sequence of numbers and letters separated by dashes into four sections of five characters each, no spaces. For example, 11AA1-11AAA-1AA11-1A111. Note that the code must be entered in Latin characters.

Enter your contact information in the lower part of the window: full name, e-mail address, and country and city of residence. This information might be requested to identify a registered user if, for example, a key is lost or stolen. If that were to happen, your contact information will enable you to obtain a new license key.

3.2.2.3. Obtaining a key file

The Settings Wizard connects to Kaspersky Lab servers and sends them your registration data (the activation code and personal information), which are inspected on the server.

If the activation code passes inspection, the Wizard receives a key file. If you install the demo version of the program, the Settings Wizard will receive a trial key file without an activation code.

The file received will be installed automatically to use the program and you will see an activation completion window with detailed information on the key being used.

If the activation code does not pass inspection, you will see a corresponding message on the screen. If this occurs, contact the software vendors from whom you purchased the program for information.

3.2.2.4. Selecting a license key file

If you have a license key file for Kaspersky Anti-Virus for Windows Servers 6.0, the Wizard will ask if you want to install it. If you do, use the **Browse** button and select the file path for the key file with the *.key* extension in the file selection window.

After you have successfully installed the key, you will see information about the license in the lower part of the window: name of the person to whom the software is registered, license number, license type (full, beta-testing, demo, etc.), and the key expiration date.

3.2.2.5. Completing program activation

The Setup Wizard will inform you that the program has been successfully activated. It will also display information on the license key installed: name of the person to whom the software is registered, license number, license type (full, beta-testing, demo, etc.), and the key expiration date.

3.2.3. Configuring update settings

Your computer's security depends directly on updating the threat signatures and program modules regularly. In this window, the Setup Wizard asks you to select a mode for program updates, and to configure a schedule.

- **Automatically**. Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scans can be set to be more frequent during virus outbreaks and less so when they are over. When Anti-Virus detects fresh updates, it downloads them and installs them on the computer. This is the default setting.
- **Every 2 hour(s)**.Updates will run automatically according to the schedule created. You can configure the schedule by clicking **Change**.
- **Manually**. If you choose this option, you will run program updates yourself.

Note that the threat signatures and program modules included with the software may be outdated by the time you install the program. That is why we recommend downloading the latest program updates. To do so, click **Update now**. Then Kaspersky Anti-Virus for Windows Servers will download the necessary updates from the update servers and will install them on your computer.

If you want to configure updates (set up network properties, select the resource from which updates will be downloaded, set up running task under a certain account or enable update distribution option), click **Settings**.

3.2.4. Configuring a virus scan schedule

Scanning selected areas of your computer for malicious objects is one of the key steps in protecting your computer.

When you install Kaspersky Anti-Virus for Windows Servers, three default virus scan tasks are created. In this window, the Setup Wizard asks you to choose a scan task setting:

Startup objects

Kaspersky Anti-Virus scans startup objects automatically when it is started by default. You can edit the schedule settings in another window by clicking **Change**.

Critical Areas

To scan critical areas of your computer automatically (system memory, Startup objects, boot sectors, Windows Server system folders) for viruses, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting for this automatic scan is disabled.

My Computer

For a full virus scan of your computer to run automatically, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting, for scheduled running of this task, is disabled. However, we recommend running a full virus scan of the server immediately after installing the program.

3.2.5. Restricting program access

Kaspersky Anti-Virus gives you the option of password-protecting the program, since several people may use the same computer, and since malicious programs could potentially disable protection. Using a password can protect the program from unauthorized attempts to disable protecting or change settings.

To enable password protection, check ☑ **Enable password protection** and complete the **Password** and **Confirm password** fields.

Select the area below that you want password protection to apply to:

- ◉ **All operations (except notifications of dangerous events)**. Request password if the user attempts any action with the program, except for responses to notifications on detection of dangerous objects.
- ◉ **Selected operations:**
  - ☑ **Saving program settings** – request password when a user attempts to save changes to program settings.
  - ☑ **Exiting the program** – request password if a user attempts to exit the program.
  - ☑ **Stopping/pausing protection components or virus scan tasks** – request password if user attempts to pause or fully disable any protection component or virus scan task.

3.2.6. Finishing the Setup Wizard

In the last window of the wizard, you will see a message saying that the program has been installed and configured successfully. You can start the application immediately by checking ☑ **Start product**.

If something went wrong during installation, such as an incompatibility problem with other antivirus applications, you will be asked to restart your computer.

3.3. Installing the program from the command prompt

To install Kaspersky Anti-Virus 6.0 for Windows Servers, enter this at the command prompt:

```
msiexec /i <package_name>
```

The Installation Wizard will start (see 3.1 on pg. 22). Once the program is installed, you must restart the computer.

To install the application non-interactively (without running the Installation Wizard), enter:

```
msiexec /i <package_name> /qn
```

This option will require you to reboot your machine manually once the installation is complete. To perform an automatic reboot from the command line, enter:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Please note that an automatic reboot will occur in non-interactive mode (using /qn key).

To install the application with an uninstall password, enter:

`msiexec /i <package_name> KLUNINSTPASSWD=******`, when performing an interactive installation;

`msiexec /i <package_name> KLUNINSTPASSWD=****** /qn`, when performing a non-interactive installation without system reboot;

`msiexec /i <package_name> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, when performing a non-interactive installation with system reboot;

If you install Kaspersky Anti-Virus in noninteractive mode, you can access the file *setup.ini*, which contains the general settings for application installation (see A.4 on pg. 176), the configuration *install.cfg* (see 13.7 on pg. 164), and the license key file. Note that these files must be located in the same folder as the Kaspersky Anti-Virus installer package.

3.4. Procedure for installing the Group Policy Object

This feature is supported on computers running Microsoft Windows 2000 Server or higher.

Using **Group Policy Object Editor**, you can install, update, and uninstall Kaspersky Anti-Virus on enterprise workstations within the domain without using Kaspersky Administration Kit.

3.4.1. Installing the program

To install Kaspersky Anti-Virus:

1. Create a shared folder on the computer that is the domain controller and copy the Kaspersky Anti-Virus *.msi* installer package to it.

   You can also copy in the file *setup.ini*, which contains the general settings for application installation (see A.4 on pg. 176), the configuration *install.cfg* (see 13.7 on pg. 164), and the license key file.

2. Open **the Group Policy Object Editor** via MMC (for more detailed information on using Group Policy Object, consult help in Microsoft Windows Server).

3. Create a new package. To do so, from the console tree, select **Group Policy Object/ Computer Configuration/ Software Settings/ Software installation** and use the command **New/ Package** from the context menu.

   In the window that opens, specify the path to the shared folder with the Anti-Virus installer (see 1). Select **Assign** from the **Select Deployment Method** dialog box and click **OK**.

The group policy will be enforced on each workstation the next time the computer is registered in the domain. Kaspersky Anti-Virus will then be installed on all computers.

3.4.2. Upgrading the program

To upgrade Kaspersky Anti-Virus:

1. Copy the installer package containing the Kaspersky Anti-Virus update in *.msi* format to the shared folder.
2. Open **Group Policy Object Editor** and created a new package using the steps given above.
3. Select the new package and select the **Properties** command from the context menu. In the package properties window, go to the **Upgrades** tab and specify the package that contains the installer for the previous version of Kaspersky Anti-Virus. To install the Kaspersky Anti-Virus upgrade and keep your protection settings, select a variant of upgrading the previous version.

The group policy will be enforced on each workstation the next time the computer is registered in the domain.

Note that Kaspersky Anti-Virus on computers running Microsoft Windows 2000 Server cannot be upgraded using Group Policy Object Editor.

3.4.3. Uninstalling the program

To uninstall Kaspersky Anti-Virus:

1. Open **Group Policy Object Editor**.
2. To do so, from the console tree, select **Group Policy Object/ Computer Configuration/ Software Settings/ Software installation**.

   Select the Kaspersky Anti-Virus package from the list. Open the context menu and select the command **All Tasks/ Remove**.

   In the **Remove Software** dialog box, select **Immediately uninstall the software from users and computers** for Kaspersky Anti-Virus to be uninstalled the next time a computer restarts.

3.5. Upgrading from 5.0 to 6.0

If Kaspersky Anti-Virus 5.0 for Windows File Servers is installed on your server, you can upgrade it to Kaspersky Anti-Virus 6.0 for Windows Servers.

After you start the Kaspersky Anti-Virus 6.0 installation program, you will be given the choice of first uninstalling the already installed version 5.0 of the

product. When the program has been uninstalled, you must restart your computer and installation of version 6.0 will then begin.

Warning!

If you are installing Kaspersky Anti-Virus 6.0 for Windows Servers from a password-protected network folder over a previous version of the program, please take note of the following. After uninstalling version 5.0 of the application and restarting your computer, the installation program will not allow you to access the network folder where the application installer package is located. This will result in the program installation being interrupted. To install the program correctly, only run the installer from a local folder.

CHAPTER 4. PROGRAM INTERFACE

Kaspersky Anti-Virus for Windows Servers has a straightforward, user-friendly interface. This chapter will discuss its basic features:

- System tray icon (see 4.1 on pg. 35)
- Context menu (see 4.2 on pg. 36)
- Main window (see 4.3 on pg. 37)
- Program settings window (see 4.4 on pg. 39)

4.1. System tray icon

As soon as you install Kaspersky Anti-Virus for Windows Servers, icon for it will appear in the system tray.

The icon is an indicator for Kaspersky Anti-Virus for Windows Servers functions. It reflects the state of protection and shows a number of basic functions performed by the program.

If the icon is active (color), this means that your computer is being protected. If the icon is inactive (black and white), this means that real-time protection is disabled.

The Kaspersky Anti-Virus for Windows Servers icon changes in relation to the operation being performed:

	A file that you or some program is opening, saving, or running is being scanned.
	Kaspersky Anti-Virus threat signatures and program modules are being updated.
	An error has occurred in some Kaspersky Anti-Virus component.

The icon also provides access to the basics of the program interface: the context menu (see 4.2 on pg. 36) and the main window (see 4.3 on pg. 37).

To open the context menu, right-click on the program icon.

To open the Kaspersky Anti-Virus for Windows Servers main window at the **Protection** section (this is the default first screen when you open the program), double-click the program icon. If you single-click the icon, the main window will open at the section that was active when you last closed it.

4.2. The context menu

You can perform basic protection tasks from the context menu (see Figure 1).

Figure 1. The context menu

The Kaspersky Anti-Virus for Windows Servers menu contains the following items:

Scan My Computer – start full computer scan. The files on all drives, including removable storage media, will be scanned.

Virus scan… – selects objects and starts scanning them for viruses. The default list contains a number of files, such as system memory, the Startup folder, email databases, all the drives on your computer, etc. You can add to the list, select files to be scanned, and start virus scans.

Update – start program modules and threat signatures update and install them on your computer.

Activate… – activate the program. You must activate your version of Kaspersky Internet Security to obtain registered user status which provides access to the full functionality of the application and Technical Support. This menu item is only available if the program is not activated.

Settings… – view and configure settings for Kaspersky Anti-Virus for Windows Servers.

Open Kaspersky Anti-Virus – open the main program window (see 4.3 on pg. 37).

Pause Protection / Resume Protection – temporarily disable or enable File Anti-Virus (see 2.2.1 on pg. 16). This menu item does not affect program updates or virus scan tasks.

Exit – close Kaspersky Anti-Virus for Windows Servers (when this option is selected, the application will be unloaded from the computer's RAM).

If a virus search task is running, the context menu will display its name with a percentage progress meter. By selecting the task, you can open the report window to view current performance results.

4.3. Main program window

The Kaspersky Anti-Virus for Windows Servers main window (see Figure 2) can be logically divided into two parts:

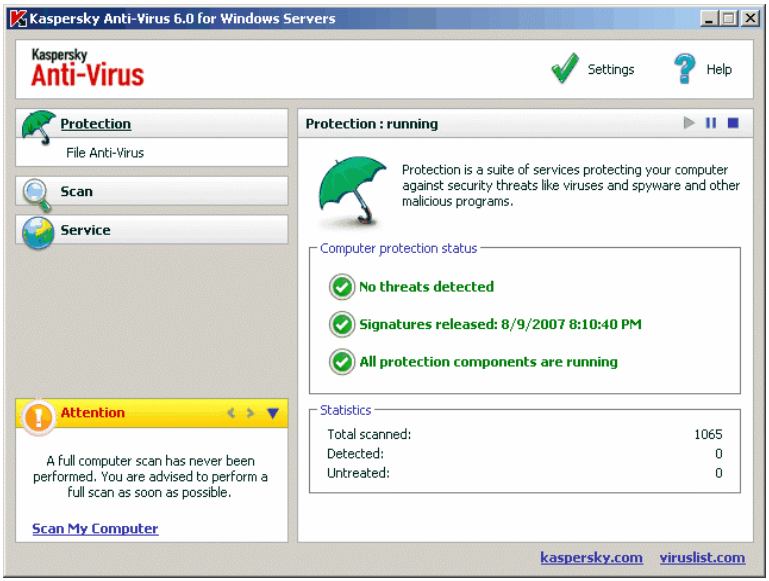
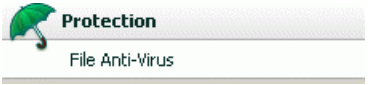
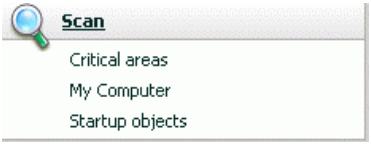
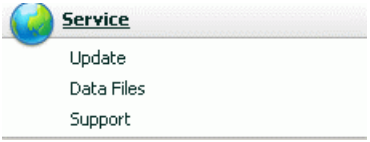
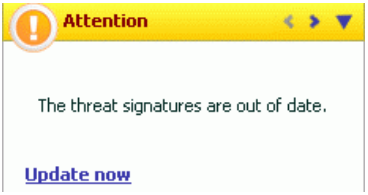


Figure 2. Kaspersky Anti-Virus for Windows Servers main window

- the left part of the window, the navigation panel, guides you quickly and easily to any component, virus scan and update task performance, or the program's support tools;
- the right part of the window, the information panel, contains information on the protection component selected in the left part of the window and displays settings for each of them, giving you tools to carry out virus scans, work with quarantined files and backup copies, manage license keys, and so on.

After selecting a section in the left part of the window, you will find information in the right-hand part that matches your selection.

We will now examine the elements in the main window's navigation panel in greater detail.

Main Window Section	Purpose
This window mostly informs you of the protection status of your computer. The **Protection** section is designed for exactly that. 	Here you will find general information about Kaspersky Anti-Virus for Windows Servers operations, allowing you to verify that everything is running correctly and examine the general statistics.
To scan your computer for malicious files or programs, use the special **Scan** section in the main window. 	This section contains a list of objects that can be scanned for viruses. The commonest and most important tasks are included in the section. These include virus scan tasks for critical areas, for startup programs, and a full computer scan.
The **Service** section includes additional Kaspersky Anti-Virus for Windows Servers features. 	Here you can update the application, view reports on running and completed tasks and components, and work with quarantined and backup objects, information on technical support, and the license key manager.
The **Comments and tips** section accompanies you as you use the application. 	In this section, you can always read tips on raising the level of protection on your server. You will also find comments about the current performance of the application and its settings.

Each element of the navigation panel is accompanied by a special context menu. The menu contains points for File Anti-Virus and tools that help the user quickly configure them, manage them, and view reports. There is an additional menu item for virus scan and update tasks that allows you to create your own task, by modifying a copy of an existing task.

You can change the appearance of the program by creating and using your own graphics and color schemes.

4.4. Program settings window

You can open the Kaspersky Anti-Virus for Windows Servers settings window from the main window (see 4.3 on pg. 37). To do so, click Settings in the upper part of it.

The settings window (see Figure 3) is similar in layout to the main window:

- the left part of the window gives you quick and easy access to the settings for each of File Anti-Virus, virus scan and update tasks, and program tools;
- the right part of the window contains a detailed list of settings for the item selected in the left part of the window.

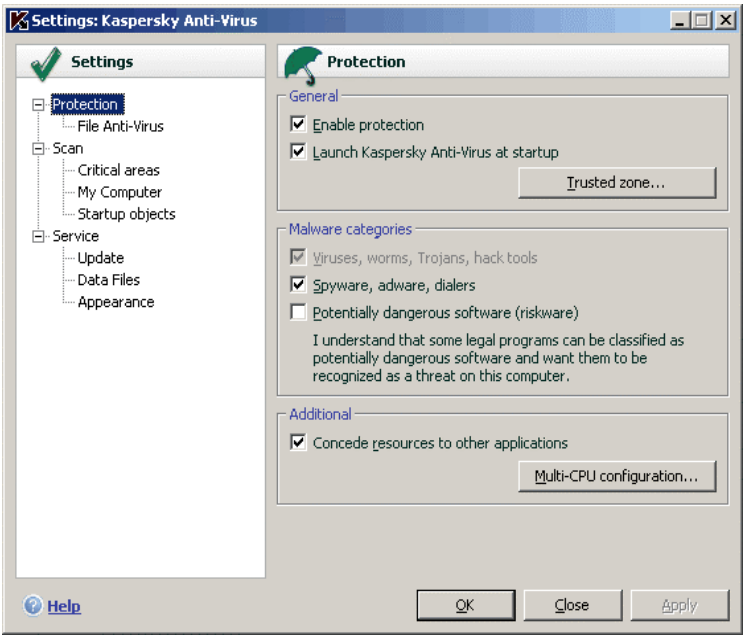


Figure 3. Kaspersky Anti-Virus for Windows Servers settings window

When you select any section, component, or task in the left part of the settings window, the right part will display its basic settings. To configure advanced settings, you can open second and third level settings windows. You can find a detailed description of program settings in the appropriate sections hereof.

CHAPTER 5. GETTING STARTED

One of Kaspersky Lab's main goals in creating Kaspersky Anti-Virus for Windows Servers was to provide optimum configuration for each of the program's options.

To make getting started easier, we have combined all the preliminary configuration stages in one Setup Wizard (see 3.2 on pg. 25) that starts as soon as the program is installed. By following the Wizard's instructions, you can activate the program, configure settings for updates and virus scans, and password-protect access to the program.

After installing and starting the program, we recommend that you take the following steps:

- Check the current protection status (see 5.1 on pg. 41) to make sure that Kaspersky Anti-Virus for Windows Servers is running at the appropriate level.
- Update the program (see 5.5 on pg. 48) if the Settings Wizard did not do so automatically after installing the program.
- Scan the computer (see 5.2 on pg. 46) for viruses.

5.1. What is the protection status of my computer?

Composite information on your computer's protection is provided in the main program window, in the **Protection** section. The *current protection status* of the computer and the *general performance statistics* of the program are displayed here.

Protection status displays the current state of protection for your computer using special indicators (see 5.1.1 on pg. 41). Statistics (see 5.1.2 on pg. 44) analyses the current program session.

5.1.1. Protection indicators

Protection status is determined by three indicators (see Figure 4), each of which reflect a different aspect of your computer's protection at any given moment, and indicate any problems in program settings and performance.

Each indicator has three possible appearances:

– *the situation is normal*; the indicator is showing that your computer's protection is adequate, and that there are no problems in the program settings or performance.

Computer protection status
No threats detected
Signatures released: 8/9/2007 8:10:40 PM
All protection components are running

Figure 4. Indicators reflecting the computer protection status

– *there are one or more deviations* in Kaspersky Anti-Virus for Windows Servers performance from the recommended level of performance, which could affect information security. Please pay heed to the actions recommended by Kaspersky Lab, which are given as links.

– *the computer's security status is critical*. Please follow the recommendations closely to improve your computer's protection. The recommended actions are given as links.

We will now examine protection indicators and the situations that each of them indicate in more detail.

The first indicator reflects the situation with malicious files and programs on your computer. The three values of this indicator mean the following:

	No threats detected Kaspersky Anti-Virus for Windows Servers has not detected any dangerous files or programs on your computer.
	All threats have been neutralized Kaspersky Anti-Virus for Windows Servers has treated all infected files and programs, and deleted those that could not be treated.
	Threats have been detected Your computer is at risk of infection. Kaspersky Anti-Virus for Windows Servers has detected malicious programs (viruses, Trojans, worms, etc.) that must be neutralized. To do so, use the Neutralize all link. Click the Details link to see more detailed information about the malicious objects.

The second indicator shows the effectiveness of your computer's protection. The indicator takes one of the following values:

	Signatures released: (date, time) Both the application and the threat signatures used by Kaspersky Anti-Virus for Windows Servers are most recent versions.
	Signatures are out of date The program modules and Kaspersky Anti-Virus for Windows Servers threat signatures have not been updated for several days. You are running the risk of infecting your computer with new malicious programs that have appeared since you last updated the program. We recommend updating Kaspersky Anti-Virus for Windows Servers. To do so, use the Update link.
	Signatures are partially corrupted The threat signature files are partially corrupted. If this occurs, it is recommended to run program updates again. If you encounter the same error message again, contact the Kaspersky Lab Technical Support Service.
	Please restart your computer You must restart your system for the program to run correctly. Save and close all files that you are working with and use the Restart computer link.
	Program updates are disabled The threat signature and program module update service is disabled. To maintain real-time protection, we recommend enabling updates.
	Signatures are obsolete Kaspersky Anti-Virus for Windows Servers has not been updated for some time. You are putting the data at great risk. Update the program as soon as possible. To do so, use the Update link.
	Signatures are corrupted The threat signature files are fully damaged. If this occurs, it is recommended to run program updates again. If you encounter the same error message again, contact the Kaspersky Lab Technical Support Service.

The third indicator shows the current functionality of the program. The indicator takes one of the following values:

	All protection components are running Kaspersky Anti-Virus for Windows Servers is protecting your computer on all channels by which malicious programs could penetrate.
	Protection is not installed When Kaspersky Anti-Virus for Windows Servers was installed, none of the monitoring components were installed. This means you can only scan for viruses. For maximum security, you should install protection components on your computer.
	All protection components are paused The protection component has been paused. To restore the component, select **Resume protection** from the context menu by clicking on the system tray icon.
	All protection components are disabled Protection is fully disabled. The protection component is not running. To restore the component, select **Resume protection** from the context menu by clicking on the system tray icon.
	Some protection components have malfunctioned The Kaspersky Anti-Virus component has experienced internal errors. If this occurs, you are advised to enable the component or restart the computer, as it is possible that the component drivers have to be registered after being updated.

5.1.2. Kaspersky Anti-Virus for Windows Servers component status

To determine how Kaspersky Anti-Virus for Windows Servers is guarding your file system, or to view the progress of a virus scan task or threat signature update, simply open the corresponding section of the main program window.

For example, to view the current File Anti-Virus status, select **File Anti-Virus** from the left-hand panel of the main window. The right-hand panel will display a summary of information about the component's operation.

For File Anti-Virus, the right-hand panel contains the **status bar**, the **Status** box and the **Statistics** box.

For File Anti-Virus, the *status bar* appears as follows:

- *File Anti-Virus : running* – file protection is active for the level selected (see 7.1 on pg. 67).
- *File Anti-Virus : paused* – File Anti-Virus is disabled for a set period of time. The component will resume operation automatically after the assigned period has expired or after the program is restarted. You can also resume file protection manually, by clicking the button located on the status bar.
- *File Anti-Virus : stopped* – the component has been stopped by the user. You can resume file protection manually, by clicking the button located on the status bar.
- *File Anti-Virus : not running* – file protection is not available for some reason.
- *File Anti-Virus : disabled (error)* – the component encountered an error.

  If a component encounters an error, try restarting it. If restart should result in an error, review component report which might contain the reason for the failure. If you are unable to troubleshoot the issue on your own, save the component report to a file using **Action** → **Save As** and contact Kaspersky Lab Technical Support.

The settings that the component uses to operate are given in the **Status** section:

- *File Anti-Virus* – current component status (running, not running, paused, etc.).
- *Security level* – the total set of parameters for component operation according to which the program protects files. By default, the **Recommended** security level will be selected, which only scans objects on the file system that are subject to infection. For example, executable (.exe) files.
- The *action* taken when a malicious object is detected.

There is no **Status** box for virus scan and update tasks. The security level, the action applied to dangerous programs for virus scan tasks, and the run mode for updates are listed in the **Settings** box.

The **Statistics** box contains information on the operation of protection components, updates, or virus scan tasks.

5.1.3. Program performance statistics

Program statistics can be found in the **Statistics** box of the main window's **Protection** section (see Figure 5), and display general information on computer protection, recorded from the time that Kaspersky Anti-Virus for Windows Servers was installed.

Figure 5. The program's general statistics box

You can left-click anywhere in the box to view a report with detailed information. The tabs display:

- Information on objects found (see 11.3.2 on pg. 117) and the status assigned to them
- Event log (see 11.3.3 on pg. 118)
- General scan statistics (see 11.3.4 on pg. 119) for your computer
- Program performance settings (see 11.3.5 on pg. 120)

5.2. How to scan your server for viruses

After installation, the program will without fail inform you using message in the lower left-hand corner of the program window that the server has not yet been scanned and will recommend that you scan it for viruses immediately.

Kaspersky Anti-Virus includes a preset default task for a computer virus scan. It is located in the **Scan** section of the program's main window.

After you select the task **My Computer** you will be able to view statistics for the most recent computer scan and task settings: what protection level was selected and what actions will be taken for dangerous objects.

To scan your computer for malicious programs,

1. Open main program window and select the task **My computer** in the **Scan** section.
2. Click the **Scan** button.

As a result, the program will start scanning your server, and the details will be shown in a special window. When you click the **Close** button, the window with information about installation progress will be hidden; this will not stop the scan.

5.3. How to scan critical areas of the computer

It is extremely important to protect these critical areas so that your computer keeps running. There is a special virus scan task for these areas, which is located in the program's main window in the **Scan** section.

After selecting the task **Critical Areas** you will be able to view statistics for the most recent computer scan and task settings: statistics for the most recent scan of these areas; task settings; what level of protection was selected, and what actions are applied to security threats. Here you can also select which critical areas you want to scan, and immediately scan those areas.

To scan critical areas of your computer for malicious programs,

1. Open main program window and select the task **Critical Areas** in the **Scan** section.
2. Click the **Scan** button.

When you do this, a scan of the selected areas will begin, and the details will be shown in a special window. When you click the **Close** button, the window with information about installation progress will be hidden; this will not stop the scan.

5.4. How to scan a file, folder or disk for viruses

Sometimes it is necessary to scan individual objects for viruses but not the entire computer: for example, one of the hard drives. You can select an object for scanning with the standard tools of the Microsoft Windows Server operating system (for example, in the **Explorer** program window, on your **Desktop**, etc.).

To scan an object,

Place the cursor over the name of the selected object, open the Microsoft Windows Server context menu by right-clicking, and select **Scan for viruses** (see Figure 6).

A scan of the selected object will then begin, and the details will be shown in a special window. When you click the Close button, the window with information about installation progress will be hidden; this will not stop the scan.

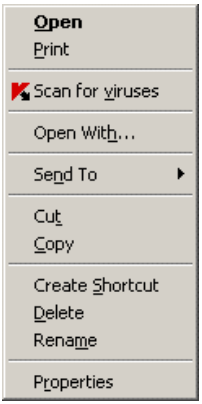


Figure 6. Scanning an object selected using
a standard Microsoft Windows Server context-sensitive menu

5.5. How to update the program

Kaspersky Lab updates the threats signatures and modules for Kaspersky Anti-Virus for Windows Servers using dedicated update servers.

Kaspersky Lab's update servers are the Kaspersky Lab Internet sites where the program updates are stored.

Warning!

You will need a connection to the Internet to update Kaspersky Anti-Virus for Windows Servers.

By default, Kaspersky Anti-Virus for Windows Servers automatically checks for updates on the Kaspersky Lab servers. If the server has the latest updates, Kaspersky Anti-Virus will download and install them in silent mode.

To update Kaspersky Anti-Virus for Windows Servers manually,

select the **Update** component in the **Service** section of the main program window and click the **Update now!** button in the right-hand part of the window.

As a result, Kaspersky Anti-Virus for Windows Servers will begin the update process, and display the details of the process in a special window.

5.6. What to do if protection is not running

If problems or errors arise in the performance of File Anti-Virus, be sure to check its status. If its status is *not running* or *error in operation*, try restarting the application.

If the problem is not solved after restarting the program, we recommend correcting potential errors using the application restore feature (**Start → Programs → Kaspersky Anti-Virus 6.0 for Windows Servers → Modify, Restore, or Remove**).

If the application restore procedure does not help, contact Kaspersky Lab Technical Support. You may need to save a report on component operation or the entire application to file and send it to Technical Support for further study.

To save the report to file:

1. Select File Anti-Virus in the **Protection** section of the main window of the program and left-click anywhere in the **Statistics** box.
2. Click the **Save As** button and in the window that opens specify the file name for the component's performance report.

To save a report on startup or the status of all Kaspersky Anti-Virus components at once (File Anti-Virus, virus scan tasks, support features):

1. Select the **Protection** section in the main window of the program and left-click anywhere in the **Statistics** box.

   or

   Click All reports in the report window for any component. Then the **Reports** tab will list reports for all program components.
2. Click the **Save As** button and in the window that opens specify a file name for the program's performance report.

CHAPTER 6. PROTECTION MANAGEMENT SYSTEM

Kaspersky Anti-Virus for Windows Servers lets you multi-task computer security management:

- Enable, disable, and pause (see 6.1 on pg. 50) the program
- Define the types of dangerous programs (see 6.2 on pg. 54) against which Kaspersky Anti-Virus for Windows Servers will protect your computer
- Create an exclusion list (see 6.3 on pg. 55) for protection
- Create your own virus scan and update tasks (see 6.4 on pg. 61).
- Configure a virus scan schedule (see 6.5 on pg. 62).
- Configure productivity settings (see 6.6 on pg. 64) for computer protection

6.1. Stopping and resuming protection on your computer

By default, Kaspersky Anti-Virus boots at startup and protects your computer the entire time you are using it. The words *Kaspersky Anti-Virus 6.0* in the upper right-hand corner of the screen let you know this. File Anti-Virus (see 2.2.1 on pg. 16) is running.

You can disable the protection provided by Kaspersky Anti-Virus for Windows Servers.

Warning!

Kaspersky Lab strongly recommends that you **do not disable protection**, since this could lead to an infection on your computer and consequent data loss.

Note that in this case protection is discussed in the context of File Anti-Virus. Disabling or pausing it does not affect the performance of virus scan tasks or program updates.

6.1.1. Pausing protection

Pausing protection means temporarily disabling File Anti-Virus.

To pause a Kaspersky Anti-Virus for Windows Servers operation:

1. Select **Pause protection** in the program's context menu (see 4.2 on pg. 36).
2. In the **Pause protection** window that opens (see Figure 7), select how soon you want protection to resume:
   - **In <time interval>** –protection will be enabled after this amount of time. To select a time value, use the drop-down menu.
   - **At next program restart** – protection will resume if you open the program from the Start Menu or after you restart your computer (provided the program is set to start when the computer is turned on (see 6.1.5 on pg. 54).
   - **By user request only** – protection will stop until you start it yourself. To enable protection, select **Resume protection** from the program's context menu.

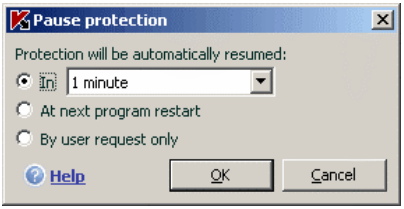


Figure 7. Pause protection window

> Tip:
>
> You can also stop protection on your computer with one of the following methods:
>
> - Click the ❚❚ button in the Protection section.
> - Select Exit from the context menu. In this case the program will be unloaded from the computer's memory.

If you pause protection, File Anti-Virus will be paused. This is indicated by:

- Inactive (gray) name of File Anti-Virus in the **Protection** section of the main window.

- Inactive (gray) system tray icon.
- The third protection indicator (see 5.1.1 on pg. 41) on your computer, which shows that **All protection components are paused**.

6.1.2. Stopping server protection

Stopping protection means fully disabling File Anti-Virus. Virus scans and updates continue to work in this mode.

If protection is stopped, it can be only be resumed by the administrator: File Anti-Virus will not automatically resume after system or program restarts. Remember that if Kaspersky Anti-Virus for Windows Servers is somehow in conflict with other programs installed on your computer, you can pause File Anti-Virus or create an exclusion (see 6.3 on pg. 55) list.

To stop all protection:

1. Open the Kaspersky Anti-Virus settings window and select the **Protection** section.
2. Uncheck **Enable protection**.

After disabling protection, File Anti-Virus will stop. This is indicated by:

1. Inactive (gray) name of File Anti-Virus in the **Protection** section of the main window.
2. Inactive (gray) system tray icon.
3. The third protection indicator (see 5.1.1 on pg. 41) on your computer, which shows that **All protection components are disabled**.

6.1.3. Pausing / stopping protection

There are several ways to stop File Anti-Virus, a virus scan, or update. Before doing so, you are strongly advised to establish why you need to stop them. It is likely that the problem can be solved in another way, for example, by changing the security level. If, for example, you are working with a database that you are sure does not contain viruses, simply add its files as an exclusion (see 6.3 on pg. 55).

To pause File Anti-Virus, virus scans, and update tasks:

Select the component or task from the left-hand part of the main window and click the button on the status bar.

The component/task status will change to ***paused***. The component or task will be paused until you resume it by clicking the ▶ button.

When you pause the component or a task, statistics for the current Kaspersky Anti-Virus session are saved and will continue to be recorded after the component is updated.

To stop the protection component or tasks:

Click the ■ button on the status bar. You can also stop the component in the program settings window by deselecting the ☑ **Enable <component name>** checkbox in the **General** section.

The component/task status will then change to *stopped (disabled)*. The component or task will be stopped until you enable it by clicking the ▶ button. For virus scans and update tasks, you will have the choice of the following options: continue the task that was interrupted, or restart it from the beginning.

When you stop the component or a task, all the statistics from previous work are cleared and when the component is started they are recorded over.

6.1.4. Restoring protection on your computer

If at some point you paused or stopped protection on your computer, you can resume it using one of the following methods:

- *From the context menu*.

  To do so, select **Resume protection**.

- *From the program's main window*.

  To do so, click the ▶ button on the status bar in the **Protection** section of the main window.

The protection status immediately changes to *running*. The program's system tray icon becomes active (color). The third protection indicator (see 5.1.1 on pg. 41) will also inform you that ✔ **All protection components are enabled**.

6.1.5. Shutting down the program

If you have to shut down Kaspersky Anti-Virus for Windows Servers, select **Exit** from the program's context menu (see 4.2 on pg. 36). This will close the program, leaving your computer unprotected.

After closing the program, you can enable computer protection again by opening Kaspersky Anti-Virus for Windows Servers (**Start→ Programs → Kaspersky Anti-Virus 6.0 for Windows Servers → Kaspersky Anti-Virus 6.0 for Windows Servers**).

You can also resume protection automatically after restarting your operating system. To enable this feature, select the **Protection** section in the program settings window and check ☑ **Launch Kaspersky Anti-Virus at startup**.

6.2. Types of malicious programs to be monitored

Kaspersky Anti-Virus for Windows Servers protects you from various types of malicious programs. Regardless of your settings, the program always protects your computer against the most dangerous types of malicious programs such as viruses, Trojans, and hack tools. These programs can do significant damage to your computer. To make your computer more secure, you can expand the list of threats that the program will detect by making it monitor additional types of dangerous programs.

To choose what malicious programs Kaspersky Anti-Virus for Windows Servers will protect you from, select the **Protection** section in the program settings window (see 4.4 on pg. 39).

The **Malware categories** box contains threat types (see 1.1 on pg. 9):

- ☑ **Viruses, worms, Trojans, hack tools**. This group combines the most common and dangerous categories of malicious programs. This is the minimum admissible security level. Per recommendations of Kaspersky Lab experts, Kaspersky Anti-Virus always monitors this category of malicious programs.
- ☑ **Spyware, adware, dialers**. This group includes potentially dangerous software that may inconvenience the user or incur serious damage.
- ☑ **Potentially dangerous software (riskware)**. This group includes programs that are not malicious or dangerous. However, under certain circumstances they could be used to cause harm to your computer.

The groups listed above comprise the full range of threats that the program detects when scanning objects.

If all groups are selected, Kaspersky Anti-Virus for Windows Servers provides the fullest possible anti-virus protection for your computer. If the second and third groups are disabled, the program will only protect you from the most common malicious programs. This does not include potentially dangerous programs and others that could be installed on your computer and could damage your files, steal your money, or take up your time.

Kaspersky Lab does not recommend disabling monitoring for the second group. If a situation arises when Kaspersky Anti-Virus classifies a program that you do not consider dangerous as a potentially dangerous program, we recommend creating an exclusion for it (see 6.3 on pg. 55).

6.3. Creating a trusted zone

A *trusted zone* is a list of objects created by the administrator that Kaspersky Anti-Virus for Windows Servers does not monitor. In other words, it is a set of programs excluded from protection.

The administrator creates a protected zone based on the properties of the files he uses and the programs installed on his computer. You might need to create such an exclusion list if, for example, Kaspersky Anti-Virus for Windows Servers blocks access to an object or program and you are sure that the file or program is absolutely safe.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects according to Virus Encyclopedia classification (the status that the program assigns to objects during a scan).

Warning!

Excluded objects are not subject to scans when the disk or folder where they are located is scanned. However, if you select that object in particular, the exclusion rule will not apply.

In order to create an exclusion list,

1. Open the application settings window and select the **Protection** section.
2. Click the **Trusted Zone** button in the **General** section.

Configure exclusion rules for objects and create a list of trusted applications in the window that opens (see Figure 8).

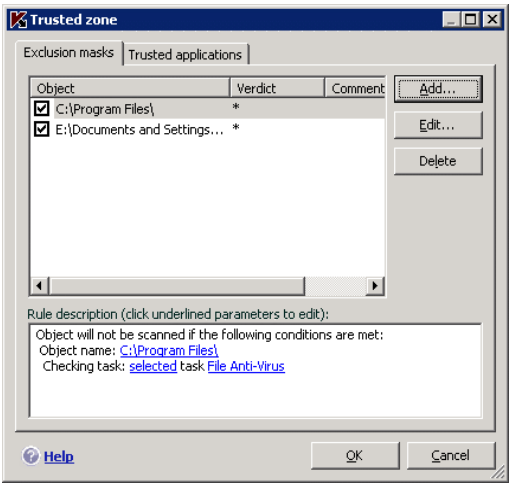


Figure 8. Creating a trusted zone

6.3.1. Exclusion rules

Exclusion rules are sets of conditions that Kaspersky Anti-Virus for Windows Servers uses to determine not to scan an object.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area, such as a folder or a program, program processes, or objects according to their Virus Encyclopedia classification.

The *verdict* is the status that Kaspersky Anti-Virus assigns to an object during the scan. A status is assigned based on classification of malicious and potentially dangerous programs founded in the Kaspersky Lab Virus Encyclopedia.

Potentially dangerous software does not have a malicious function but can be used as an auxiliary component for a malicious code, since it contains holes and errors. This category includes, for example, remote administration programs, IRC clients, FTP servers, all-purpose utilities for stopping or hiding processes, keyloggers, password macros, autodialers, etc. These programs are not classified as viruses. They can be divided into several types, e.g. Adware, Jokes, Riskware, etc. (for more information on potentially dangerous programs detected by Kaspersky Anti-Virus for Windows Servers, see the Virus Encyclopedia at www.viruslist.com). After the scan, these programs may be blocked. Since several of them are very common, you have the option of excluding them from the scan. To do so, you must add the name or threat mask of the object to the trusted zone using the Virus Encyclopedia classification.

For example, imagine you use a Remote Administrator program frequently in your work. This is a remote access system with which you can work from a remote computer. Kaspersky Anti-Virus for Windows Servers views this sort of application activity as potentially dangerous and may block it. To keep the application from being blocked, you must create an exclusion rule that specifies not-a-virus:RemoteAdmin.Win32.RAdmin.22 as a verdict.

When you add an exclusion, a rule is created that File Anti-Virus and virus scan tasks can later use. You can create exclusion rules in a special window that you can open from the program settings window, from the notice about detecting the object, and from the report window.

*To add exclusions on the **Exclusion mask** tab:*

1. Click on the **Add** button in the **Exclusion mask** tab.
2. In the window that opens (see Figure 9), click the exclusion type in the **Properties** section:

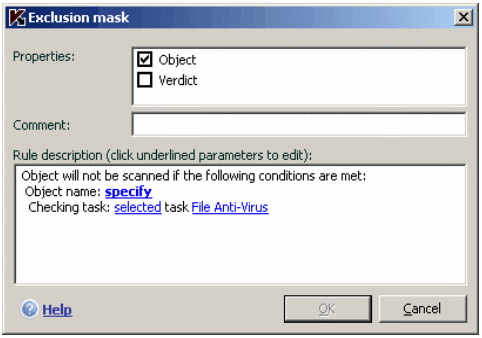


Figure 9. Creating an exclusion rule

Object – exclusion of a certain object, directory, or files that match a certain mask from scans.

Verdict – excluding an object from the scan based on its status from the Virus Encyclopedia classification.

If you check both boxes at once, a rule will be created that object with a certain status according to Virus Encyclopedia classification. In such a case, the following rules apply:

- If you specify a certain file as the **Object** and a certain status in the **Verdict** section, the file specified will only be an exclusion if during the scan it is classified as the threat selected.
- If you select an area or folder as the **Object** and the status (or mask) as the **Verdict**, then objects with that status will only be excluded from the scan in that area or folder.

3. Assign values **to** the selected exclusion types. To do so, left-click in the **Rule description** section on the specify link located next to the exclusion type:

   - For the **Object** type, enter its name in the window that opens (this can be a file, a particular folder, or a file mask (see A.2 on pg. 175). Check ☑ **Include subfolders** for the object (file, file mask, folder) to be recursively excluded from the scan.
   - Enter the full name of the threat that you want to exclude from scans as given in the Virus Encyclopedia or use a mask for the **Verdict** (see A.3 on pg. 175).

     For some classification objects, you can assign advanced conditions for applying rules in the **Advanced settings** field.

4. Define which Kaspersky Anti-Virus for Windows Servers components will use this rule. If the selected option is any, this rule will apply to all components. If you want to restrict the rule to one or several components, click on any, which will change to selected. In the window that opens, check the boxes for the components that you want this exclusion rule to apply to.

To create an exclusion rule from a program notice stating that it has detected a dangerous object:

1. Use the Add to trusted zone link in the notification window.
2. In the window that opens, be sure that all the exclusion rule settings match your needs. The program will fill in the object name and threat type automatically, based on information from the notification. To create the rule, click **OK**.

To create an exclusion rule from the report window:

1. Select the object in the report that you want to add to the exclusions.
2. Open the context menu and select **Add to Trusted zone** (see Figure 10).

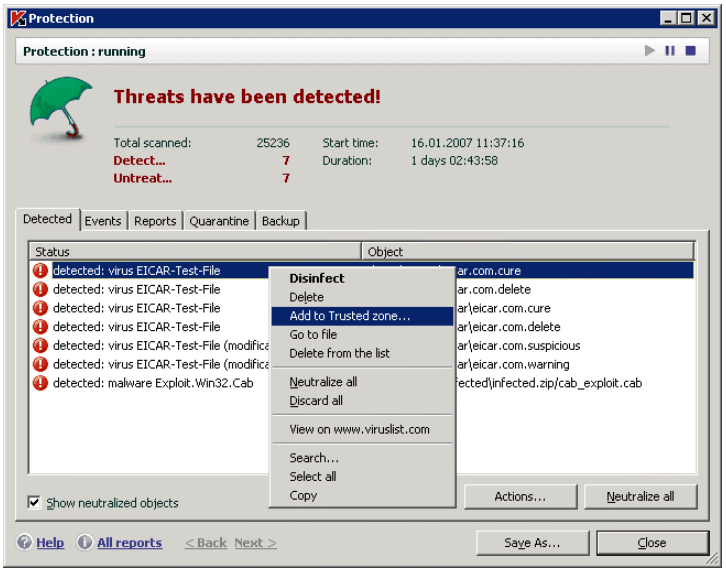


Figure 10. Creating an exclusion rule from report

6.3.2. Trusted applications

Kaspersky Anti-Virus for Windows Servers can create a list of trusted applications that need not have their file activity monitored, suspicious or otherwise.

For example, you feel that objects and processes used by Windows Server **Notepad** are safe and do not need to be scanned. To exclude objects used by this process from scanning, add **Notepad** to the trusted applications list. However, the executable file and the trusted application process will be scanned for viruses as before. To fully exclude the application from scanning, you must use exclusion rules (see 6.3.1 on pg. 56).

In addition, some actions classified as dangerous are perfectly normal features for a number of programs. For example, keyboard layout toggling programs regularly intercept text entered on your keyboard. To accommodate such programs and stop monitoring their activity, you are advised to add them to the trusted application list.

Excluding trusted applications can also solve potential compatibility conflicts between Kaspersky Anti-Virus for Windows Servers and other applications (for example, network traffic from another computer that has already been scanned by the anti-virus application) and can boost computer productivity.

By default, Kaspersky Anti-Virus for Windows Servers scans objects opened, run, or saved by any program process.

You can create a list of trusted applications on the special **Trusted applications** tab (see Figure 11). By default the trusted applications list contains a list of applications that will not be monitored based on Kaspersky Lab recommendations when you install Kaspersky Anti-Virus. If you do not trust an application on the list, deselect the corresponding checkbox. You can edit the list using the **Add**, **Edit**, and **Delete** buttons on the right.

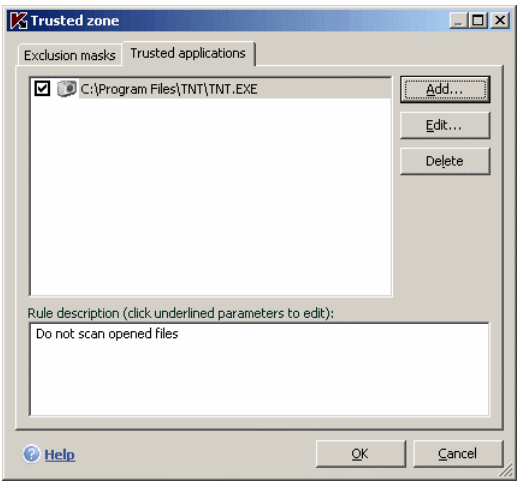


Figure 11. Trusted application list

To add a program to the trusted application list:

1. Click the **Add** button on the right-hand part of the **Trusted applications** tab.
2. In the **Trusted application** window (see Figure 12) that opens, select the application using the **Browse** button. A context menu will open, and by clicking **Browse** you can go to the file selection window and select the path to the executable file, or by clicking **Applications** you can go to a list of applications currently running and select them as necessary.

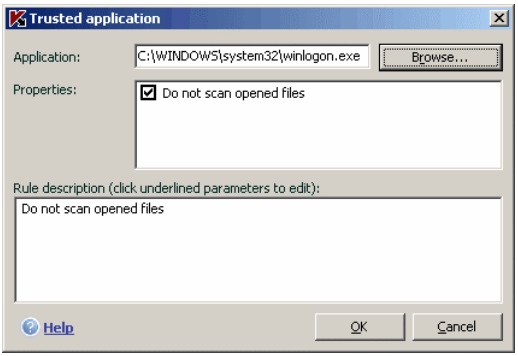


Figure 12. Adding an application to the trusted list

When you select a program, Kaspersky Anti-Virus for Windows Servers records the internal attributes of the executable file and uses them to identify the trusted program during scans.

The file path is inserted automatically when you select its name.

3. Next, if necessary, specify which actions performed by this process will not be monitored by Kaspersky Anti-Virus:

   Do not scan opened files – excludes from the scan all files that the trusted application process.

6.4. Starting tasks under another profile

Kaspersky Anti-Virus for Windows Servers 6.0 has a feature that can start scan tasks under another user profile. This feature is by default disabled, and tasks are run under the profile under which you are logged into the system.

The feature is useful if for example, you need access rights to a certain object during a scan. By using this feature, you can configure tasks to run under another user profile that has the necessary privileges.

Program updates may be made from a source to which you do not have access (for example, the network update folder) or authorized user rights for a proxy server. You can use this feature to run the Updater with another profile that has those rights.

To configure a scan task that starts under a different user profile:

1. Select the task name in the **Scan** section (for virus scans) or the **Service** section (for update tasks) of the main window and use the Settings link to open the task settings window.
2. Click the **Settings** button in the task settings window and go to the **Additional** tab in the window that opens (see Figure 13).
3. To enable this feature, check **Run this task as**. Enter the data for the login that you want to start the task as below: user name and password.

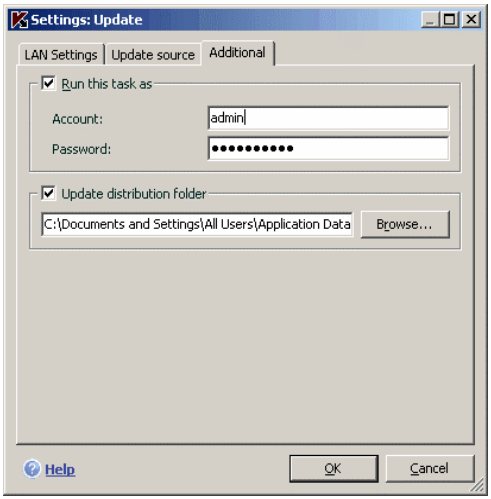


Figure 13. Configuring an update task from another profile

6.5. Configuring Scheduled Tasks and Notifications

Schedule settings are identical for virus scan tasks, application updates, and Kaspersky Anti-Virus event notifications.

By default, the virus scan tasks created at application install are disabled. Startup objects are the exception since they are scanned every time Kaspersky Anti-Virus is started. Updates are configured to occur automatically by default as updates become available on Kaspersky Lab update servers.

In the event that you are not satisfied with these settings, you may reconfigure the scheduling. Select a task by name under **Virus Scan** (for virus scan tasks) or

Service (for updates and update distribution) and open the related settings window by clicking Settings.

To have tasks start according to a schedule, check the automatic task start box in the **Run Mode** section. You can edit the times for starting the scan task in the **Schedule** window (see Figure 14), that opens when you click **Change**.

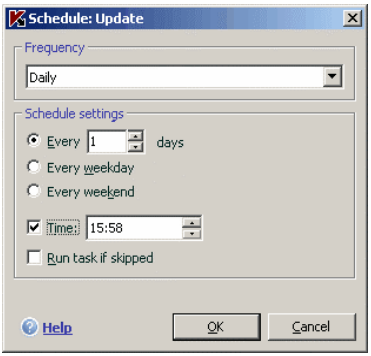


Figure 14. Configuring a task schedule

The primary setting to define is the frequency of an event (task execution or notification). Select the desired option under **Frequency** (see Figure 14). Then, settings for the selected option are to be specified under Schedule Settings. The following options are available:

- **Time.** Start a task or send a notification at the specified date and time.
- **At Application Startup.** Run task or send notification every time Kaspersky Anti-Virus starts. A time delay may also be specified relative to the start of the application for a task to be run.
- **After every update.** Task is run after each threat signature update (this option only applies to virus scan tasks).
- **Minutes.** The time interval between scans or notifications will be several minutes. Specify the length of time in minutes under schedule settings. It should not exceed 59 minutes.
- **Hours.** The interval between scans or notifications is several hours. If this option is selected, specify the time interval under schedule settings: **Every N hours** and specify *N*. Enter **Every 1 hour**, for instance, if you want the task to run hourly.
- **Days.** The task is started or the notification is sent at an interval of several days. Specify the interval in the schedule settings:
  - Select **Every n days** and enter a value for n if you wish to maintain an interval of several days. Select **Every Weekday**, if you want the task to run daily Monday through Friday.

- Select **Every Weekend** to run the task or send notification on Saturdays and Sundays only.

  Use the **Time** field to specify what time of day the scan task will be run.

Weeks. The task is started or the notification sent on certain days of the week. If you select this option, put checkmarks next to the days of the week on which you need the task to run. Enter time of day in the **Time** field.

Months. The task is started or the notification sent once a month at a specified time.

If a task cannot run for some reason (an email program is not installed, for example, or the computer was shut down at the time), the task can be configured to run automatically as soon as it becomes possible. Check **Run Task if Skipped** in the schedule window.

6.6. Power options

Virus scans increase the load on the central processor and disk subsystems, thereby slowing down other programs. By default, if such a situation arises, the application pauses virus scans and frees up system resources for user applications.

However, there are a number of programs that can be launched as soon as the processor's resources are freed and run in background mode. If you do not want virus scans to depend on the operation of such programs, uncheck **Concede resources to other applications** (see Figure 15).

Note that this setting can be configured individually for every virus scan task. If you choose to do this, the configuration for a specific task has a higher priority.

In the window that opens when click the **Multi-CPU configuration** button, you can assign settings for Kaspersky Anti-Virus for running on a multi-processor server (see 6.7 on pg. 65).

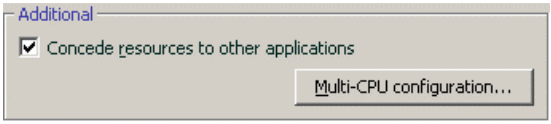


Figure 15. Configuring power settings

To configure power settings:

Select the **Protection** section of the main program window and click the Settings link. Configure power settings in the **Additional** box.

6.7. Multi-processor server configuration

In this window, you can configure settings for server productivity when using a multi-processor configuration.

Number of anti-virus kernel instances – number of copies of the anti-virus kernel to be loaded when Anti-Virus Kaspersky is running on the server. This number determines the number of antivirus processes running in parallel.

The more copies of the antivirus engine that are running, the faster anti-virus operations are processed. However, this affects the overall performance of the server.

In addition, running several antivirus processes on the server simultaneously ensures that the server is always protected in the event that one of the engines experiences an error.

To distribute antivirus processes between server processors automatically, check ☑ **Use special driver to manage parallel processes**.

If this checkbox is deselected, you can manually regulate the load on the server, for example, reserving a portion of the processors for antivirus processing and portions of the server's direct tasks. To do so, deselect the processors that dedicated to the server in the **Utilized processors** box.

Kaspersky Lab recommends reserving at least one processor for server tasks when running on a multiprocessor server.

CHAPTER 7. ANTI-VIRUS PROTECTION OF THE SERVER FILE SYSTEM

Kaspersky Anti-Virus includes *File Anti-Virus*, which protects your computer files against infection. It loads when you start your operating system, runs in your computer's RAM, and scans all files that are opened, saved, or executed.

The component's activity is indicated by the Kaspersky Anti-Virus for Windows Servers system tray icon, which looks like this whenever a file is being scanned.

File Anti-Virus by default scans only *new or modified files,* that is, only files that have been added or changed since the previous scan. Files are scanned with the following algorithm:

1. The component intercepts attempts by users or programs to access any file.
2. File Anti-Virus scans the iChecker™ and iSwift™ databases for information on the file intercepted. A decision is made whether to scan the file based on the information retrieved.

The scanning process includes the following steps:

1. The file is analyzed for viruses. Malicious objects are detected by comparison with the program's *threat signatures*, which contain descriptions of all malicious programs and threats known to date, with methods for neutralizing them.
2. After the analysis, there are three available courses of action:
    a. If malicious code is detected in the file, File Anti-Virus blocks the file, places a copy of it in *Backup*, and attempts to disinfect the file. If the file is successfully disinfected, it becomes available again. If not, the file is deleted.
    b. If code is detected in a file that appears to be, but is not definitely, malicious, the file is sent to *Quarantine*.
    c. If no malicious code is discovered in the file, it is immediately restored.

7.1. Selecting a file security level

File Anti-Virus protects files that you are using at one of the following levels (see Figure 16):

- **High** – the level with the most comprehensive monitoring of files opened, saved, or run.
- **Recommended** – Kaspersky Lab recommends this settings level. It will scan the following object categories:
    - Programs and files by contents
    - New objects and objects modified since the last scan
    - Embedded OLE objects
- **Low** – level with settings that let you comfortably use applications that require significant system resources, since the scope of files scanned is reduced.

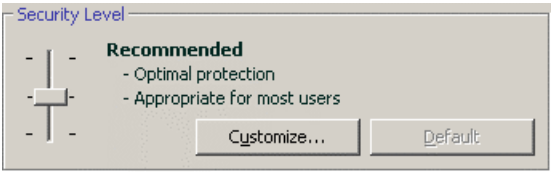


Figure 16. File Anti-Virus security level

The default setting for File Anti-Virus is **Recommended**.

You can raise or lower the protection level for files you use by either selecting the level you want, or changing the settings for the current level.

To change the security level:

Adjust the sliders. By adjusting the security level, you define the ratio of scan speed to the total number of files scanned: the fewer files are scanned for viruses, the higher the scan speed.

If none of the set file security levels meet your needs, you can customize the protection settings. To do so, select the level that is closest to what you need as a starting point and edit its settings. In such a case, the level will be set at **Custom**. Let's look at an example of when user defined file security levels could be useful.

Example:

The work you do on your computer uses a large number of file types, and some the files may be fairly large. You would not want to run the risk of skipping any files in the scan because of the size or extension, even if this would somewhat affect the productivity of your computer.

Tip for selecting a level:

Based on the source data, one can conclude that you have a fairly high risk of being infected by a malicious program. The size and type of the files being handled is quite varied and skipping them in the scan would put your data at risk. You want to scan the files you use by contents, not by extension.

You are advised to start with the **Recommended** security level and make the following changes: remove the restriction on scanned file sizes and optimize File Anti-Virus operation by only scanning new and modified files. Then the scan will not take up as many system resources so you can comfortably use other applications.

To modify the settings for a security level:

Click the **Settings** button in the File Anti-Virus settings window. Edit the File Anti-Virus settings in the window that opens and click **OK**.

As a result, a fourth security level will be created, **Custom**, which contains the protection settings that you configured.

7.2. Configuring File Anti-Virus

Your settings determine how File Anti-Virus will defend your computer. The settings can be broken down into the following groups:

- Settings that define what file types (see 7.2.1 on pg. 69) are to be scanned for viruses
- Settings that define the scope of protection (see 7.2.2 on pg. 71)
- Settings that define how the program responds to dangerous objects (see 7.2.5 on pg. 75)
- additional File Anti-Virus settings (see 7.2.3 on pg. 73)

The following sections will examine these groups in detail.

7.2.1. Defining the file types to be scanned

When you select file types to be scanned, you establish what file formats, sizes, and what drives will be scanned for viruses when opened, executed, or saved.

To make configuration easier, all files are divided into two groups: *simple* and *compound*. Simple files, for example, .txt files, do not contain any objects. Compound objects can include several objects, each of which may in turn contain other objects. There are many examples: archives, files containing macros, spreadsheets, emails with attachments, etc.

The file types scanned are defined in the **File types** section (see Figure 17). Select one of the three options:

- **Scan all files**. With this option selected, all file system objects that are opened, run, or saved will be scanned without exceptions.
- **Scan programs and documents (by contents)**. If you select this group of files, File Anti-Virus will only scan potentially infected files – files that a virus could imbed itself in.

  > Note:
  >
  > There are a number of file formats that have a fairly low risk of having malicious code injected into them and subsequently being activated. An example would be .txt files.
  >
  > And vice versa, there are file formats that contain or can contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of injection and activation of malicious code in such files is fairly high.

  Before searching for viruses in a file, its internal header is analyzed for the file format (txt, doc, exe, etc.). If the analysis shows that the file format cannot be infected, it is not scanned for viruses and is immediately returned to the user. If the file format can be infected, the file is scanned for viruses.
- **Scan programs and documents (by extension)**. If you select this option, File Anti-Virus will only scan potentially infected files, but the file format will be determined by the filename's extension. Using the extension link, you can review a list of file extensions (see A.1 on pg. 172) that are scanned with this option.

Tip:

Do not forget that someone could send a virus to your computer with an extension (e.g. .txt) that is actually an executable file renamed as a .txt file. If you select **Scan programs and documents (by extension)**, the scan would skip such a file. If **Scan programs and documents (by contents)** is selected, the extension is ignored, and analysis of the file headers will uncover that the file is an .exe file. File Anti-Virus would scan the file for viruses.

In the **Productivity** section, you can specify that only new files and those that have been modified since the previous scan should be scanned for viruses. This mode noticeably reduces scan time and increases the program's performance speed. To select this mode, check **Scan new and changed files only**. This mode applies to both simple and compound files.

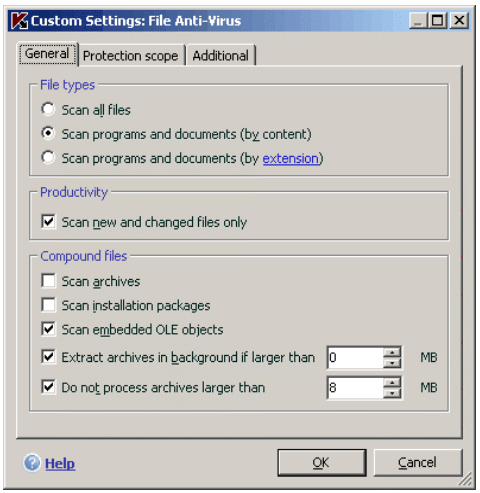


Figure 17. Selecting file types to scan

In the **Compound files** section, specify which compound files to scan for viruses:

- **Scan all/only new archives** – scans .zip, .cab, .rar, and .arj archives.
- **Scan all/only new installation packages** – scans self-extracting archives for viruses.
- **Scan all/only new embedded OLE objects** – scans objects embedded in files (for example, Microsoft Office Excel spreadsheets or macros imbedded in a Microsoft Office Word file, email attachments, etc.).

You can select and scan all files, or only new files, for each type of compound file. To do so, left-click the link next to the name of the object to toggle its value. If the **Productivity** section has been set up only to scan new and modified files, you will not be able to select the type of compound files to be scanned.

To specify compound files that should not be scanned for viruses, use the following settings:

- **Extract archives in background if larger than... MB**. If the size of a compound object exceeds this restriction, the program will scan it as a single object (by analyzing the header) and will make it available again. The objects that it contains will be scanned later. If this option is not checked, access to files larger than the size indicated will be blocked until they have been scanned.
- **Do not process archives larger than... MB**. With this option checked, files larger than the size specified will be skipped by the scan.

7.2.2. Defining protection scope

By default, File Anti-Virus scans all files when they are used, regardless of where they are stored, whether it be a hard drive, CD/DVD-ROM, or flash drive.

You can limit the scope of protection. To do so:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Settings** button and select the **Protection Scope** tab (see Figure 18) in the window that opens.

The tab displays a list of objects that File Anti-Virus will scan. Protection is enabled by default for all objects on hard drives, removable media, and network drives connected to your computer. You can add to and edit the list using the **Add, Edit,** and **Delete** buttons.

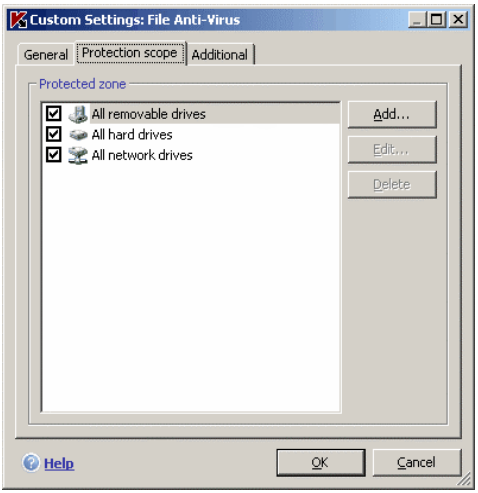


Figure 18. Created a protected zone

If you want to protect fewer objects, you can do so using the following methods:

- Specify only folders, drives, and files that need to be protected.
- Create a list of objects that do not need to be protected (see 6.3 on pg. 55).
- Combine methods one and two – create a protection scope that excludes a number of objects.

You can use masks when you add objects for scanning. Note that you can only enter masks will absolute paths to objects:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** - all files in folder *C:\dir*
- **C:\dir*.exe** - all files with the extension .exe in the folder *C:\dir*
- **C:\dir*.ex?** – all files with the extension .ex? in the folder *C:\dir*, where ? can represent any one character
- **C:\dir\test** – only the file *C:\dir\test*

In order for the scan to be carried out recursively, check ☑ **Include subfolders**.

Warning!

Remember that File Anti-Virus will scan only the files that are included in the protection scope created. Files not included in that scope will be available for use without being scanned. This increases the risk of infection on your computer.

7.2.3. Configuring advanced settings

As additional File Anti-Virus settings, you can specify the file system scanning mode and configure the conditions for temporarily pausing the component.

To configure additional File Anti-Virus settings:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking the Settings link.
2. Click the **Customize** button and select the **Additional** tab in the window that opens (see Figure 19).

The file scanning mode determines the File Anti-Virus processing conditions. You have following options:

- **Smart mode**. This mode is aimed at speeding up file processing and return them to the user. When it is selected, a decision to scan is made based on analyzing the operations performed with the file.

  For example, when using a Microsoft Office file, Kaspersky Anti-Virus scans the file when it is first opened and last closed. All operations in between that overwrite the file are not scanned.

  Smart mode is the default.

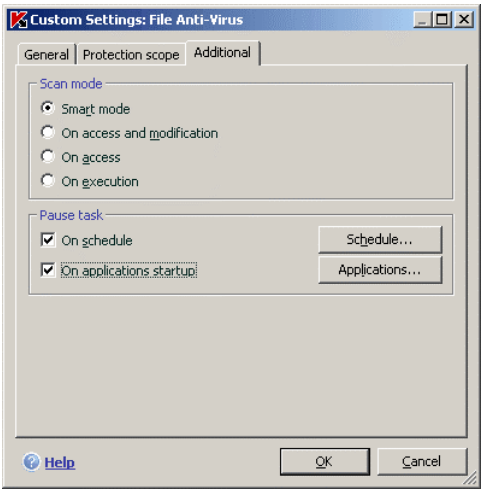


Figure 19. Configuring advanced File Anti-Virus settings

- **On access and modification** – File Anti-Virus scans files as they are opened or edited.

- **On access** – only scans files when an attempt is made to open them.
- **On execution** – only scans files when an attempt is made to run them.

You might need to pause File Anti-Virus when performing tasks that require significant operating system resources. To lower the load and ensure that the user regains access to files quickly, we recommend configuring the component to disable at a certain time or while certain programs are used.

To paused the component, check **On schedule** and select a time frame for stopping and starting the component in the window that opens (see Figure 20) when you click the **Schedule** button. To do so, enter a value in the format HH:MM in the corresponding fields.

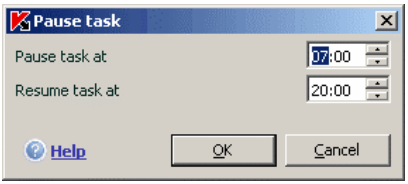


Figure 20. Pausing the component

To disable the component when working with programs that require significant resources, check **On applications startup** and edit the list of programs in the window that opens (see Figure 21) by clicking **Applications**.

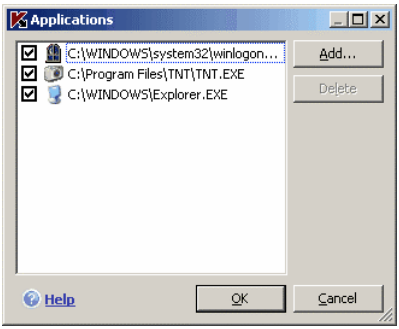


Figure 21. Creating an application list

To add an application to the list, use the **Add** button. A context menu will open, and by clicking **Browse** you can go to the standard file selection window and specify the executable file the application to add. Alternatively, go to the list of applications currently running from the **Applications** item and select the one you want.

To delete an application, select it from a list and click **Delete**.

You can temporarily disable the pause on File Anti-Virus when using a specific application. To do so, uncheck the name of the application. You do not have to delete it from the list.

7.2.4. Restoring default File Anti-Virus settings

When configuring File Anti-Virus, you can always return to the default performance settings. Kaspersky Lab considers them to be optimal and has combined them in the **Recommended** security level.

To restore the default File Anti-Virus settings:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Default** button in the **Security Level** section.

If you modified the list of objects included in the protected zone when configuring File Anti-Virus settings, the program will ask you if you want to save that list for future use when you restore the initial settings. To save the list of objects, check **Protected Zone** in the **Restore Settings** window that opens.

7.2.5. Selecting actions for objects

If File Anti-Virus discovers or suspects an infection in a file while scanning it for viruses, the program's next steps depend on the object's status and the action selected.

File Anti-Virus can label an object with one of the following statuses:

- Malicious program status (for example, *virus, Trojan*) (see 1.1 on pg. 9).
- *Potentially infected*, when the scan cannot determine whether the object is infected. This means that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, all infected files are subject to disinfection, and if they are potentially infected, they are sent to Quarantine.

To edit an action for an object:

select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings. All potential actions are displayed in the appropriate sections (see Figure 22).

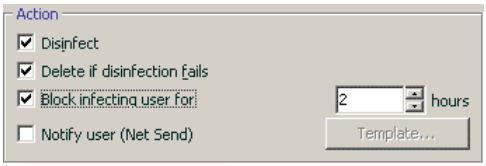


Figure 22. Possible File Anti-Virus actions with dangerous objects

If the action selected was	When a dangerous object is detected
☑ **Disinfect** ☐ **Delete if disinfection fails**	Access to the object is blocked and an attempt is made to disinfect it. A copy of the object is stored in Backup. If it is successfully disinfected, it is returned to the user for regular use. If the object could not be treated, it is moved to Quarantine. Information about this is recorded in the report. Later you can attempt to disinfect this object.
☑ **Disinfect** ☑ **Delete if disinfection fails**	Access to the object is blocked and an attempt is made to disinfect it. A copy of the object is stored in Backup. If it is successfully disinfected, it is returned to the user for regular use. If the object cannot be disinfected, it is deleted.
☐ **Disinfect** ☑ **Delete**	File Anti-Virus will block access to the object and will delete it.
☑ **Block infecting user for … hours**	Blocks access to the server or computer from which the attempt was made to copy the infected or potentially infected file. This action can additionally be applied to actions related to processing the file (disinfecting or deleting). Note that if the user exits a session and logs into the system again, Kaspersky Anti-Virus will consider this a different connect and the ban will be

If the action selected was	When a dangerous object is detected
	lifted.
☑ **Notify user (Net Send)**	Notifies the user from whose computer the attempt was made to copy the infected or potentially infected file to the server, via Net Send. To configure the notification template, click the **Template** button (see 7.2.6 on pg. 77).

When disinfecting or deleting an object, Kaspersky Anti-Virus creates a backup copy and sends it to Backup in case the object needs to be restored or an opportunity arises to treat it.

Warning! The actions **Block user** and **NetSend** are not available if you are running the application under Microsoft Windows NT Server.

7.2.6. Creating a notification template

In this window, you can format the text for the notification template for the user whose computer attempted to copy an infected/potentially infected file to the server.

The notification text may contain macros to provide more information: the path to the dangerous object and the threat name. To add macros to the notification text, click **Macros**.

To restore the initial text used for the notification template, click the **Default** button.

7.3. Postponed disinfection

In Kaspersky Anti-Virus for Windows Servers, access to infected files is blocked if they are being disinfected and if deleted in cases where they could not be disinfected or deleted.

In Kaspersky Anti-Virus for Windows Servers, access to infected files is blocked if they are being disinfected and if deleted in cases where they could not be disinfected.

In order to regain access to blocked objects, they must be disinfected. To do so:

1. Select **File Anti-Virus** in the main window of the program and left-click anywhere in the **Statistics** box.
2. Select the objects that interest you on the **Detected** tab and click the **Action → Neutralize all** button.

Successfully disinfected files will be returned to the user. Any that cannot be treated, you can *delete* or *skip* it. In the latter case, access to the file will be restored. However, this significantly increases the risk of infection on your computer. It is strongly recommended not to skip malicious objects.

CHAPTER 8. SCANNING FOR VIRUSES ON YOUR COMPUTER

Kaspersky Anti-Virus for Windows Servers can scan individual items – files, folders, disks, plug-and-play devices – or the entire computer. Scanning for viruses stops malicious code that has gone undetected by File Anti-Virus from spreading.

Kaspersky Anti-Virus for Windows Servers includes the following default scan tasks:

Critical Areas

Scans all critical areas of the computer for viruses, including: system memory, programs loaded on startup, boot sectors on the hard drive, and the *Windows* and *system32* system directories. The task aims to detect active viruses quickly on the system without fully scanning the computer.

My Computer

Scans for viruses on your computer with a thorough inspection of all disk drives, memory, and files.

Startup Objects

Scans for viruses all programs loaded when the operating system boots.

The default settings for these tasks are the recommended ones. You can edit these settings (see 8.4 on pg. 82) or create a schedule (see 6.5 on pg. 62) for running tasks.

You also have the option of creating your own tasks (see 8.3 on pg. 81) and creating a schedule for them. For example, you can schedule a scan task for email databases once per week, or a virus scan task for any **My Documents** folder.

In addition, you can scan any object for viruses without creating a special scan task. You can select an object to scan from the Kaspersky Anti-Virus for Windows Servers interface, or with the standard tools of the Windows Server operating system (for example, in the **Explorer** program window or on your **Desktop**).

You can view a complete list of virus scan tasks for your computer by clicking on **Scan** in the left-hand pane of the main application window.

8.1. Managing virus scan tasks

You can run a virus scan task manually or automatically using a schedule (see 6.5 on pg. 62).

To start a virus scan task manually:

Check the box beside the task name in the **Scan** section of the main program window, and click the button on the status bar.

The tasks currently being performed (including tasks created through Kaspersky Administration Kit) are displayed in the context menu by right-clicking on the system tray icon

To pause a scan task:

Click the button on the status bar. The task status will change to *paused*. This will pause the scan until you start the task again manually or it starts again automatically according to the schedule.

To stop a scan task:

Click the button on the status bar. The task status will change to *stopped*. This will stop the scan until you start the task again manually or it starts again automatically according to the schedule. The next time you run the task, the program will ask if you would like to continue the task where it stopped or begin it over.

8.2. Creating a list of objects to scan

To view a list of objects to be scanned for a particular task, select the task name (for example, **My computer**) in the **Scan** section of main program window. The list of objects will be displayed in the right-hand part of the window under the status bar (see Figure 23).

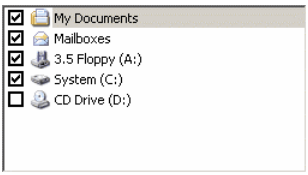


Figure 23. List of objects to scan

Object scan lists are already made for default tasks created when you install the program. When you create your own tasks or select an object for a virus scan task, you can create a list of objects.

You can add to or edit an object scan list using the buttons to the right of the list. To add a new scan object to the list, click the **Add** button, and in the window that opens select the object to be scanned.

For the user's convenience, you can add categories to a scan area such as user mailboxes, RAM, startup objects, operating system backup, and files in the Kaspersky Anti-Virus Quarantine folder.

In addition, when you add a folder that contains embedded objects to a scan area, you can edit the recursion To do so, select an object in the corresponding list, open its context menu and use **Include Subfolders** option.

To delete an object, select it from the list (when you do so, the name of the object will be highlighted in gray) and click the **Delete** button. You can temporarily disable scanning for individual objects for any task without deleting them from the list. To do so, uncheck the box beside the object that you do not want scanned.

To start a scan task, click the **Scan** button, or select **Start** from the menu that opens when you click the **Actions** button.

In addition, you can select an object to be scanned with the standard tools of the Windows Server operating system (for example, in the Explorer program window or on your Desktop, etc.) (see Figure 24). To do so, select the object, open the Windows Server context menu by right-clicking, and select **Scan for viruses**.

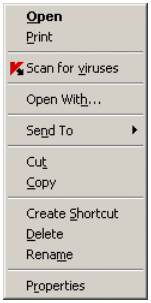


Figure 24. Scanning objects from the Windows context menu

8.3. Creating virus scan tasks

To scan objects on your computer for viruses, you can use built-in scan tasks included with the program and create your own tasks. New scan tasks are created using existing tasks that a template.

To create a new virus scan task:

1. Select the task with the settings closest to those you need, in the **Scan** section of the main program window.
2. Open the context menu by right-clicking on the task name, or click the **Actions** button to the right of the scan object list, and select **Save as...**.
3. Enter the name for the new task in the window that opens and click **OK**. A task with that name will then appear in the list of tasks in the **Scan** section of the main program window.

Warning!

There is a limit to the number of tasks that can be created. The maximum is four tasks.

The new task is a copy of the one it was based on. You need to continue setting it up by creating an scan object list (see 8.2 on pg. 80), setting up properties that govern the task (see 8.4 on pg. 82), and, if necessary, configuring a schedule (see 6.5 on pg. 62) for running the task automatically.

To rename a created task:

Select the task in the **Scan** section of the main program window. Right-click on the task's name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Rename**.

Enter the new name for the task in the window that opens and click **OK**. The task name will also be changed in the **Scan** section.

To delete a created task:

Select the task in the **Scan** section of the main program window. Right-click on the task's name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Delete**.

You will be asked to confirm that that you want to delete the task. The task will then be deleted from the list of tasks in the **Scan** section.

Warning!

You can only rename and delete tasks that you have created.

8.4. Configuring virus scan tasks

The methods are used to scan objects on your computer are determined by the properties assigned for each task.

To configure task settings:

open application settings window and select the task name in the **Scan** section.

You can use the settings window for each task to:

- Select the security level that the task will use (see 8.4.1 on pg. 83)
- Edit advanced settings:
    - define what file types are to be scanned for viruses (see 8.4.2 on pg. 84)
    - configure task start using a different user profile (see 6.4 on pg. 61)
    - configure advanced scan settings (see 8.4.5 on pg. 89)
- restore default scan settings (see 8.4.3 on pg. 87)
- select an action that the program will apply when it detects an infected or potentially infected object (see 8.4.4 on pg. 87)
- create a schedule (see 6.5 on pg. 62) to automatically run tasks.

In addition, you can configure global settings (see 8.4.6 on pg. 90) for running all tasks.

The following sections examine the task settings listed above in detail.

8.4.1. Selecting a security level

Each virus scan task can be assigned a security level (see Figure 25):

High – the most complete scan of the entire computer or individual disks, folders, or files. You are advised to use this level if you suspect that a virus has infected your computer.

Recommended – Kaspersky Lab experts recommend this level. The same files will be scanned as for the **High** setting, except for email databases.

Low – level with settings that let you comfortably use resource-intensive applications, since the scope of files scanned is reduced.

Figure 25. Selecting a virus scan security level

By default, the file scanning is set to **Recommended**.

You can raise or lower the scan security level by selecting the level you want or changing the settings for the current level.

To edit the security level:

Adjust the sliders. By adjusting the security level, you define the ratio of scan speed to the total number of files scanned: the fewer files are scanned for viruses, the higher the scan speed.

If none of the file security levels listed meet your needs, you can customize the scan settings. To do so, select the level that is closest to what you need as a starting point and edit its settings. If you do so, the level will be renamed as **Custom**.

To modify the settings for a security level:

click the **Settings** button in the task settings window. Edit the scan settings in the window that opens and click **OK**.

As a result, a fourth security level will be created, **Custom settings**, which contains the scan settings that you configured.

8.4.2. Specifying the types of objects to scan

By specifying the types of objects to scan, you establish which file formats, files sizes, and drives will be scanned for viruses when this task runs.

The file types scanned are defined in the **File types** section (see Figure 26). Select one of the three options:

- **Scan all files**. With this option, all files will be scanned without exception.
- **Scan programs and documents (by content)**. If you select this group of programs, only potentially infected files will be scanned – files into which a virus could imbed itself.

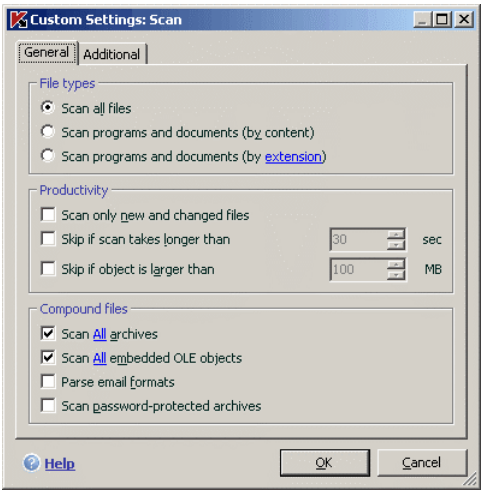


Figure 26. Configuring scan settings

> Note:
>
> There are files in which viruses cannot insert themselves, since the contents of such files does not contain anything for the virus to hook onto. An example would be .txt files.
>
> In addition, vice versa, there are file formats that contain or can contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of insertion and activation of malicious code in such files is fairly high.

Before searching for viruses in an object, its internal header is analyzed for the file format (txt, doc, exe, etc.).

- **Scan programs and documents (by extension)**. In this case, the program will only scan potentially infected files, and in doing so, the file format will be determined by the filename's extension. Using the link, you can review a list of file extensions that are scanned with this option (see A.1 on pg. 172).

> Tip:
>
> Do not forget that a virus in a file with the extension .txt could actually be an executable file renamed as a .txt file. If you select the **Scan programs and documents (by extension)** option, the scan would skip such a file. If the **Scan programs and documents (by contents)** is selected, the program will analyze file headers, discover that the file is an .exe file, and thoroughly scan it for viruses.

In the **Productivity** section, you can specify that only new files and those that have been modified since the previous scan or new files should be scanned for viruses. This mode noticeably reduces scan time and increases the program's performance speed. To do so, you must check ☑ **Scan only new and changed files**. This mode extends to simple and compound files.

You can also set time and file size limits for scanning in the **Productivity** section.

☑ **Skip if scan takes longer than... secs.** Check this option and enter the maximum scan time for an object. If this time is exceeded, this object will be removed from the scan queue.

☑ **Skip if object is larger than…MB**. Check this option and enter the maximum size for an object. If this size is exceeded, this object will be removed from the scan queue.

In the **Compound files** section, specify which compound files will be analyzed for viruses:

☑ **Scan All/Only New archives** – scan .rar, .arj, .zip, .cab, .lha, .jar, and .ice archives.

Warning!

Kaspersky Anti-Virus does not delete compressed file formats that it does not support (for example, .ha, .uue, .tar) automatically, even if you select the option of automatically curing or deleting if the objects cannot be cured.

To delete such compressed files, click the Delete archives link in the dangerous object detection notification. The screen displays this message when the **Prompt for action during the scan/ Prompt for action when the scan is complete** option is selected (see 8.4.4 on pg. 87). You can also delete infected archives manually.

☑ **Scan all/only new embedded OLE objects**– scan objects imbedded in files (for example, Excel spreadsheets or a macro imbedded in a Microsoft Word file, email attachments, etc.).

You can select and scan all files or only new ones for each type of compound file. To do so, use the link next to the name of the object. It changes its value when you left-click on it. If the **Productivity** section has been set up only to scan new and modified files, you will not be able to select the type of compound files to be scanned.

☑ **Parse email formats** – scan email files and email databases. If this checkbox is deselected, mail format files will be scanned as binary files (without dissecting the format), and if the file is not infected and the Scan all files option is selected, information with the status *OK* will be entered into the report. If file scanning settings were selected by type and extension, the object will be skipped with the verdict *excluded by type*.

Please note, when scanning password-protected email databases:

- Kaspersky Anti-Virus for Windows Servers detects malicious code in Microsoft Office Outlook 2000 databases but does not disinfect them;
- Kaspersky Anti-Virus for Windows Servers does not support scans for malicious code in Microsoft Office Outlook 2003 protected databases.

☑ **Scan password-protected archives** – scans password protected archives. With this feature, a window will request a password before scanned archived objects. If this box is not checked, password-protected archives will be skipped.

8.4.3. Restoring default scan settings

When configuring scan task settings, you can always return to the recommended settings. Kaspersky Lab considers them to be optimal and has combined them in the **Recommended** security level.

To restore the default scan settings:

1. Select the task name in the **Scan** section of the main window and use the Settings link to open the task settings window.
2. Click the **Default** button in the **Security Level** section.

8.4.4. Selecting actions for objects

If a file is found to be infected or suspicious during a scan, the program's next steps depend on the object status and the action selected.

One of the following statuses can be assigned to the object after the scan:

- Malicious program status (for example, *virus, Trojan*).
- *Potentially infected*, when the scan cannot determine whether the object is infected. It is likely that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, all infected files are disinfected, and if they are potentially infected, they are sent to Quarantine.

To edit an action for an object:

select the task name in the **Scan** of the main program window and use the Settings link to open the task settings window. The possible responses are displayed in the appropriate sections (see Figure 27).

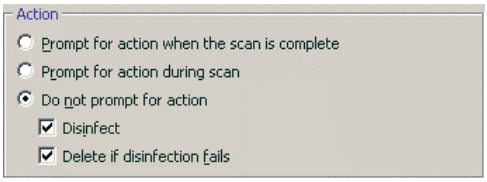

Action
Prompt for action when the scan is complete
Prompt for action during scan
Do not prompt for action
Disinfect
Delete if disinfection fails

Figure 27. Selecting actions for dangerous objects

If the action selected was	When it detects a malicious or potentially infected object
Prompt for action when the scan is complete	The program does not process the objects until the end of the scan. When the scan is complete, the statistics window will pop up with a list of objects detected one after another, requesting an action for each of the objects.
Prompt for action during scan	The program will issue a warning message containing information about what malicious code has infected or potentially infected the file, and gives you the choice of one of the following actions.
Do not prompt for action	The program records information about objects detected in the report without processing them or issuing a notification. You are advised not to use this feature, since infected and potentially infected objects stay on your computer and it is practically impossible to avoid infection.
Do not prompt for action **Disinfect**	The program attempts to treat the object detected without asking for confirmation. If the file can be disinfected, it is moved to Backup to be disinfected later. If the program cannot disinfect the object, access to it is blocked.
Do not prompt for action	The program attempts to treat the object detected without asking for

If the action selected was	When it detects a malicious or potentially infected object
☑ **Disinfect** ☑ **Delete if disinfection fails**	confirmation. If the object cannot be disinfected, it is deleted. A copy is stored in Backup.
◉ **Do not prompt for action** ☐ **Disinfect** ☑ **Delete**	The program automatically deletes the object

When disinfecting or deleting an object, Kaspersky Anti-Virus creates a backup copy and sends it to Backup (see 12.2 on pg. 143) in case the object needs to be restored or an opportunity arises to treat it.

With the status *potentially infected*, the object is moved to Quarantine without attempting to disinfect it.

8.4.5. Additional virus scan settings

In addition to configuring the basic virus scan settings, you can also use advanced settings (see Figure 28):

☑ **Enable iChecker technology** – uses technology that can increase scan speed by excluding certain objects from the scan. An object is excluded from the scan using a special algorithm that takes into account the release date of the threat signatures, the date the object was last scanned, and modifications to scan settings.

For example, you have an archived file that the program scanned and assigned the status of not infected. The next time, the program will skip this archive, unless it has been modified or the scan settings have been changed. If the structure of the archive has changed because a new object has been added to it, if the scan settings have changed, or if the threat signatures have been updated, the program will scan the archive again.

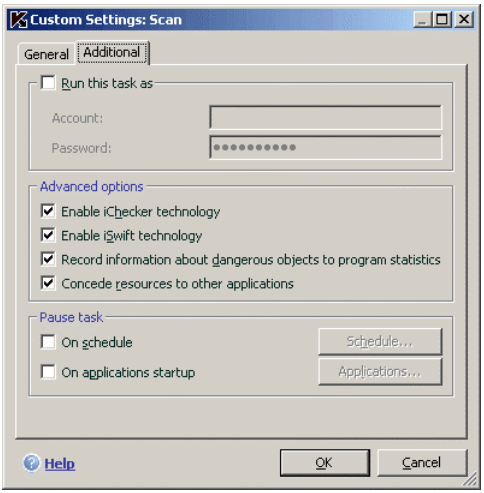


Figure 28. Advanced scan settings

There are limitations to iChecker™: it does not work with large files and only applies to objects with a structure that Kaspersky Anti-Virus for Windows Servers recognizes (for example, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **Enable iSwift technology**. This technology is a development of iChecker technology for computers using an NTFS file system. There are limitations to iSwift: it is bound to a specific location for the file in the file system and can only be applied to objects in an NTFS file system.
- **Record information about dangerous objects to program statistics** – save information about detected dangerous objects to general program statistics and display a list of threats detected during the scan on the **Detected** tab of the report (see 11.3.2 on pg. 117) window. If this option is disabled the information about dangerous objects will not be displayed in the report and it will be impossible to process data.
- **Concede resources to other applications** – pause that virus scan task if the processor is busy with other applications.

8.4.6. Setting up global scan settings for all tasks

Each scan task is executed according to its own settings. By default, the tasks created when you install the program on your computer use the settings recommended by Kaspersky Lab.

You can configure global scan settings for all tasks. You will use a set of properties used to scan an individual object for viruses as a starting point.

To assign global scan settings for all tasks:

1. Select the **Scan** section in the left-hand part of the main program window and click Settings.
2. In the settings window that opens, configure the scan settings: Select the security level (see 8.4.1 on pg. 83), configure advanced level settings, and select an action (see 8.4.4 on pg. 87) for objects.
3. To apply these new settings to all tasks, click the **Apply** button in the **Other task settings** section. Confirm the global settings that you have selected in the popup dialogue box.

CHAPTER 9. TESTING KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

After installing and configuring Kaspersky Anti-Virus, we recommend that you verify that settings and program operation are correct using a test virus and variations of it.

9.1. The EICAR test virus and its variations

The test virus was specially developed by eicar (The European Institute for Computer Antivirus Research) for testing antivirus functionality.

The test virus IS NOT A VIRUS and does not contain program code that could damage your computer. However, most antivirus programs will identify it as a virus.

Never use real viruses to test the functionality of an antivirus!

You can download the test virus from the official **EICAR** website: http://www.eicar.org/anti_virus_test_file.htm.

The file that you downloaded from the **EICAR** website contains the body of a standard test virus. Kaspersky Anti-Virus will detected, label it a **virus**, and take the action set for that object type.

To test the reactions of Kaspersky Anti-Virus when different types of objects are detected, you can modify the contents of the standard test virus by adding one of the prefixes in the table shown here.

Prefix	Test virus status	Corresponding action when the application processes the object
No prefix, standard test virus	The file contains a test virus. You cannot disinfect the object.	The application will identify the object as malicious and not subject to treatment and will delete it.
CORR–	Corrupted.	The application could access the object but could not scan it, since the object is corrupted (for example, the file structure is breached, or it is an invalid file format).
SUSP– WARN–	The file contains a test virus (modification). You cannot disinfect the object.	This object is a modification of a known virus or an unknown virus. At the time of detection, the threat signature databases do not contain a description of the procedure for treating this object. The application will place the object in Quarantine to be processed later with updated threat signatures.
ERRO–	Processing error.	An error occurred while processing the object: the application cannot access the object being scanned, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is being scanned on a network drive).
CURE–	The file contains a test virus. It can be cured. The object is subject to disinfection, and the text of the body of the virus will	The object contains a virus that can be cured. The application will scan the object for viruses, after which it will be fully cured.

Prefix	Test virus status	Corresponding action when the application processes the object
	change to CURE.	
DELE–	The file contains a test virus. You cannot disinfect the object.	This object contains a virus that cannot be disinfected or is a Trojan. The application deletes these objects.

The first column of the table contains the prefixes that need to be added to the beginning of the string for a standard test virus. The second column describes the status and reaction of Kaspersky Anti-Virus to various types of test virus. The third column contains information on objects with the same status that the application has processed.

Values in the anti-virus scan settings determine the action taken on each of the objects.

9.2. Testing File Anti-Virus

To test the functionality File Anti-Virus;

1. Create a folder on a disk, copy to it the test virus downloaded from the organization's official website (see 9.1 on pg. 92), and the modifications of the test virus that you created.
2. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors. To do so, check **Log non-critical events** in the report settings window (see 11.3.1 on pg. 117).
3. Run the test virus or a modification of it.

File Anti-Virus will intercept your attempt to access the file, will scan it, and will delete it.

When you select different preset configuration options for dealing with detected objects, you can test File Anti-Virus's reaction to detecting various object types.

You can view details on File Anti-Virus performance in the report on the component.

9.3. Testing virus scan tasks

To test Virus scan tasks:

1. Create a folder on a disk, copy to it the test virus downloaded from the organization's official website (see 9.1 on pg. 92), and the modifications of the test virus that you created.
2. Create a new virus scan task (see 8.3 on pg. 81) and select the folder containing the set of test viruses as the objects to scan (see9.1 on pg. 92).
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors. To do so, check **Log non-critical events** in the report settings window.
4. Run the virus scan task (see 8.1 on pg. 80).

When you run a scan, as suspicious or infected objects are detected, notifications will be displayed on screen will information about the objects, prompting the user for the next action to take:

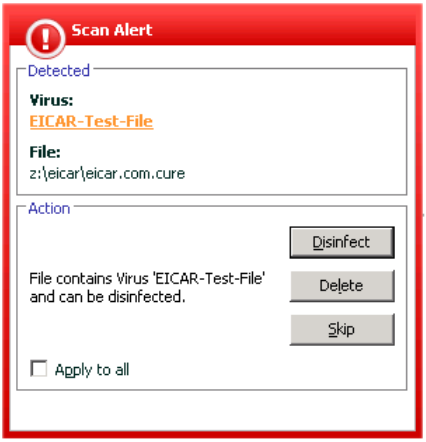


Figure 29. Dangerous object detected

This way, by selecting different preset configuration options for actions, you can test Kaspersky Anti-Virus reactions to detecting various object types.

You can view details on virus scan task performance in the report on the component.

CHAPTER 10. PROGRAM UPDATES

Keeping your anti-virus software up-to-date is an investment in security. Because new viruses, Trojans, and malicious software emerge daily, it is important to regularly update the application to keep your information constantly protected.

Updating the application involves the following components being downloaded and installed on your computer:

- **Threat Signatures**

  The application uses threat signatures to protect information on your computer. The software components that provide protection use the database of threat signatures to search for and disinfect harmful objects on your computer. The signatures are added to every hour, with records of new threats and methods to combat them. Therefore, it is recommended that they are updated on a regular basis.

  Previous versions of Kaspersky Lab applications have supported *standard* and *extended* database sets. Each database dealt with protecting your computer against different types of dangerous objects. In Kaspersky Anti-Virus for Windows Servers you don't need to worry about selecting the appropriate threat signature set. Now our products use an threat signatures that protect you from both malicious and potentially dangerous objects, and from hacker attacks.

- **Application modules**

  In addition to the signatures, you can upgrade the modules for Kaspersky Anti-Virus for Windows Servers. New application updates appear regularly.

The main update source for Kaspersky Anti-Virus for Windows Servers is Kaspersky Lab's update servers.

To download available updates from the update servers, your computer must be connected to the Internet.

If you do not have access to Kaspersky Lab's update servers (for example, your computer is not connected to the Internet), you can call the Kaspersky Lab main office at +7 (495) 797-87-00, +7 (495) 645-79-39 or +7 (495) 956-70-00 to request contact information for Kaspersky Lab partners, who can provide you with zipped updates on floppy disks or CDs.

Updates can be downloaded in one of the following modes:

- *Automatically*. Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scans can be set to be more frequent during virus outbreaks and less so when they are over. When Anti-Virus detects fresh updates, it downloads them and installs them on the computer. This is the default setting.
- *By schedule*. Updating is scheduled to start at a specified time.
- *Manually*. With this option, you launch the Updater manually.

During updating, the application compares the threat signatures and application modules on your computer with the versions available on the update server. If the server has the latest version of signatures and modules, a note will be displayed about it in the application window. If the signatures and modules on your computer differ from those on the update server, only the missing part of the updates will be downloaded. The Updater does not download threat signatures and modules that you already have, which significantly increases download speed and saves Internet traffic.

Before updating threat signatures, Kaspersky Anti-Virus for Windows Servers creates backup copies of them that can be used if a rollback (see 10.2 on pg. 98) is required. If, for example, the update process corrupts the threat signatures and leaves them unusable, you can easily roll back to the previous version and try to update the signatures later.

You can distribute the updates retrieved to a local source while updating the application (see 10.4.4 on pg. 105). This feature allows you to update databases and modules used by 6.0 applications on networked computers to conserve bandwidth.

10.1. Starting the Updater

You can begin the update process at any time. It will run from the update source that you have selected (see 10.4.1 on pg. 100).

You can start the Updater from:

- the context menu (see 4.2 on pg. 36).
- from the program's main window (see 4.3 on pg. 37)

To start the Updater from the shortcut menu:

1. Right click the application icon in the system tray to open the shortcut menu.
2. Select **Update**.

To start the Updater from the main program window:

1. Select **Update** in the **Service** section.
2. Click the **Update now!** Button in the right panel of the main window or use the ▶ button on the status bar.

The update progress will be displayed in a special window, which can be hidden by clicking **Close**. The update will continue with the window hidden.

Note that updates are distributed to the local source during the update process, provided that this service is enabled (see 10.4.4 on pg. 105).

10.2. Rolling back to the previous update

Every time you start the Updater, Kaspersky Anti-Virus for Windows Servers creates a backup copy of the current threat signatures before it starts downloading updates. This way you can return to using the previous version of signatures if an update fails.

To rollback to the previous version of threat signatures:

1. Select the **Update** component in the **Service** section of the main program window.
2. Click the **Rollback** button in the right panel of the main program window.

10.3. Creating update tasks

Kaspersky Anti-Virus has a built-in update task for updating program modules and threat signatures. You can also create your own update tasks with various settings and start schedules.

For example, you installed Kaspersky Anti-Virus on a laptop that you use at home and at your office. At home, you update the program from the Kaspersky Lab update servers, and at the office, from a local folder that stores the updates you need. Use two different tasks to avoid having to change update settings every time you change locations.

To create an advanced update task:

1. Select **Update** from the **Service** section of the main program window, open the context menu by right-clicking, and select **Save as**.

2. Enter the name for the task in the window that opens and click **OK**. A task with that name will then appear in the **Service** section of the main program window.

Warning!

There is a limit to the number of update tasks that the user can create in Kaspersky Anti-Virus. Maximum number: two tasks.

The new task inherits all the properties of the task it is based on, except for the schedule settings. The default automatic scan setting for the new task is disabled. You need to continue setting it up by specifying the update source (see 10.4.1 on pg. 99), network settings (see 10.4.3 on pg. 104), and if necessary enabling tasks with privileges (see 6.4 on pg. 61) and configuring the schedule (see 6.5 on pg. 62).

To rename a task:

Select the task from the **Service** section of the main program window, open the context menu by right-clicking, and select **Rename**.

Enter the new name for the task in the window that opens and click **OK**. The task name will then be changed in the **Service** section.

To delete a task:

Select the task from the **Service** section of the main program window, open the context menu by right-clicking, and select **Delete**.

Confirm that you want to delete the task in the confirmation window. The task will then be deleted from the list of tasks in the **Service** section.

Warning!

Rename and delete are only available for customized tasks.

10.4. Configuring update settings

The Updater settings specify the following parameters:

- The source from which the updates are downloaded and installed (see 10.4.1 on pg. 100);
- Application update mode and the specific items updated (see 10.4.2 on pg. 102);
- Update frequency if updates run on schedule (see 6.5 on pg. 62);
- Account under which the update will run (see 6.4 on pg. 61);

- The requirement to copy downloaded updates to a local directory (see 10.4.4 on pg. 105);
- What actions are to be performed after updating is complete (see 10.4.5 on pg. 106)

The following sections examine these aspects in detail.

10.4.1. Selecting an update source

The *update source* is some resource, containing updates for the threat signatures and Kaspersky Anti-Virus application modules.

You can use the following as update sources:

- *Administration server* – a centralized update repository located on the Kaspersky Administration Kit Administration Server (for more details, see the Administrator User's Guide for Kaspersky Administration Kit 6.0).
- *Kaspersky Lab's update servers* – special web sites containing available updates for the threat signatures and application modules for all Kaspersky Lab products.
- *FTP or HTTP server or local or network folder* – local server or folder that contains the latest updates.

If you cannot access Kaspersky Lab's update servers (for example, you have no Internet connection), you can call the Kaspersky Lab main office at +7 (495) 797-87-00, 7 (495) 645-79-39 or +7 (495) 956-70-00 to request contact information for Kaspersky Lab partners, who can provide zipped updates on floppy disks or CDs.

Warning!

When requesting updates on removable media, please specify whether you want to have the updates for application modules as well.

You can copy the updates from a disk and upload them to a FTP or HTTP site, or save them in a local or network folder.

Select the update source on the **Update source** tab (see Figure 30).

By default, the updates are downloaded from Kaspersky Lab's update servers. The list of addresses that this item represents cannot be edited. When updating, Kaspersky Anti-Virus for Windows Servers calls this list, selects the address of the first server, and tries to download files from this server. If updates cannot be downloaded from the first server, the application tries to connect to each of the servers in turn until it is successful.

To download updates from another FTP or HTTP site:

1. Click **Add.**
2. In the **Select Update Source** dialog box, select the target FTP or HTTP site or specify the IP address, character name, or url-address of this site in the **Source** field. When selecting an ftp site as an update source, authentication settings must be entered in the URL of the server in the format ftp://<user_name>:<password>@<host>:<port>.

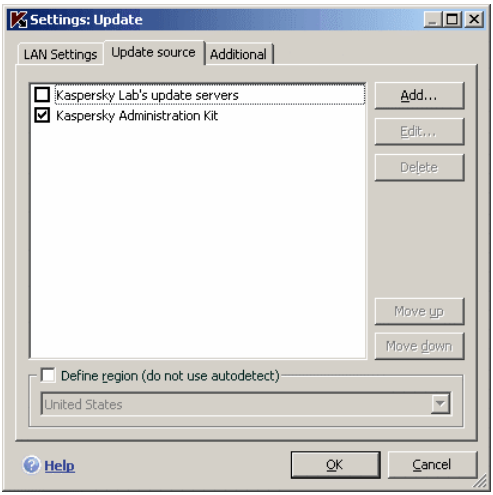


Figure 30. Selecting an update source

Warning!

If a resource located outside the LAN is selected as an update source, you must have an Internet connection to update.

To update from a local folder:

1. Click **Add.**
2. In the **Select Update Source** dialog box, select a folder or specify the full path to this folder in the **Source** field.

Kaspersky Anti-Virus for Windows Servers adds new update sources at the top of the list, and automatically enables the source, by checking the box beside the source name.

If several resources are selected as update sources, the application tries to connect to them one after another, starting from the top of the list, and retrieves

the updates from the first available source. You can change the order of sources in the list using the **Move up** and **Move down** buttons.

To edit the list, use the **Add**, **Edit** and **Remove** buttons. You cannot edit or delete is the Kaspersky Lab or Kaspersky Administration Kit update servers.

If you use Kaspersky Lab's update servers as the update source, you can select the optimal server location for downloading updates. Kaspersky Lab has servers in several countries. Choosing the Kaspersky Lab update server closest to you will save you time and download updates faster.

To choose the closest server, check ☑ **Define region (do not use autodetect)** and select the country closest to your current location from the dropdown list. If you check this box, updates will run taking the region selected in the list into account. This checkbox is deselected by default and information about the current region from the operating system registry is used.

10.4.2. Selecting an update method and what to update

When configuring updating settings, it is important to define what will be updated and what update method will be used.

Update objects (see Figure 31) are the components that will be updated:

- threat signatures
- program modules

The threat signatures are always updated, and the application modules are only updated if the settings are configured for it.

Figure 31. Selecting update objects

If you want to download and install updates for program modules:

Check ☑ **Update program modules** in the **Update** window.

If there is an application module update on the update source, the application will download the required updates and apply them after the system is restarted. Downloaded module updates will not be installed until the computer is restarted.

If the next program update occurs before the computer is restarted and the previously downloaded application module updates are installed, threat signatures only will be updated.

Update method (see Figure 32) defines how the Updater is started. In **Run mode** you can select one of these methods:

Automatically. Kaspersky Anti-Virus checks the update source for update packages at specified intervals (see 10.4.1 on pg. 99). When Anti-Virus detects fresh updates, it downloads them and installs them on the computer.

If a network resource is specified as an update source, Kaspersky Anti-Virus tries to start the Updater after a certain amount of time has elapsed as specified in the previous update packet.

If a local folder is selected as an update source, the application tries to download the updates from the local folder as often as specified in the update package that was downloaded during the previous update. This option allows Kaspersky Lab to regulate how often the program is updated in case of virus outbreaks and other potentially dangerous situations. Your application will receive the latest updates for the threat signatures, network attacks, and software modules in a timely manner, thus preventing malicious software to penetrate the server.

Figure 32. Selecting an update run mode

By schedule. Updating is scheduled to start at a specified time. By default, scheduled updates will occur every 2 hours. To edit the default schedule, click the **Change...** button near the mode title and make the necessary changes in the window that opens (for more details, see 6.5 on pg. 62). This mode is used by default.

Manually. With this option, you start the Updater manually. Kaspersky Anti-Virus for Windows Servers notifies you when it needs to be updated:

- First, a pop-up message informing you that updating is required appears above the application icon in the system tray (if notices are enabled; see 11.8.1 on pg. 128);
- The second indicator in the main program window informs you that your computer is out-of-date (see 5.1.1 on pg. 41)
- A recommendation, that the application needs updating, appears in the message section in the main program window (see 4.3 on pg. 37)

10.4.3. Configuring connection settings

If you set up the program to retrieve updates from Kaspersky Lab's update servers, or from other FTP or HTTP sites, you are advised to first check your connection settings.

All settings are grouped on a special tab – **LAN Settings** (see Figure 33).

Check **Use passive FTP mode if possible** if you download the updates from an FTP server in passive mode (for example, through a firewall). If you are working in active FTP mode, clear this checkbox.

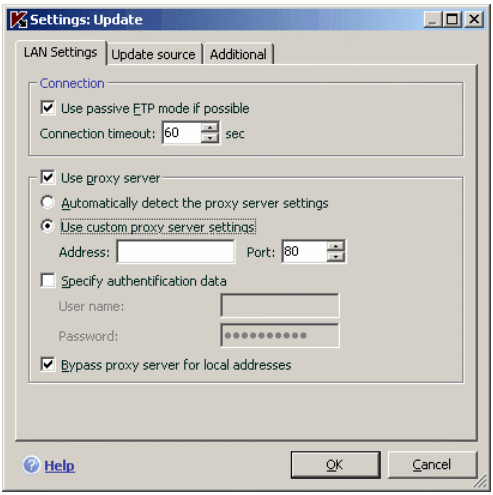


Figure 33. Configuring network update settings

In the **Connection timeout (sec)** field, assign the time allotted for connection with the update server. If the connection fails, once this time has elapsed the program will attempt to connect to the next update server. This continues until a connection is successfully made or until all the available update servers are attempted.

Check **Use proxy server** if you are using a proxy server to access the Internet and, if necessary, select the following settings:

- Select the proxy server settings that will be used during updating:

  Automatically detect the proxy server settings. If you select this option, the proxy settings are detected automatically using WPAD (Web Proxy Auto-Discovery Protocol). If this protocol cannot detect

the address, Kaspersky Anti-Virus will use the proxy server settings specified in Microsoft Internet Explorer.

Use custom proxy settings – Use a proxy that is different from that specified in the browser connection settings. In the **Address** field, enter either the IP address or the symbolic name of the proxy server, and specify the number of the proxy port in the **Port** field.

- Specify whether authentication is required on the proxy server. *Authentication* is the process of verifying user registration data for access control purposes.

  If authentication is required to connect to the proxy server, check **Specify authentification data** and specify the username and password in the fields below. In this event, first NTLM authentication and then BASIC authentication will be attempted.

  If this checkbox is not selected or if the data is not entered, NTLM authentication will be attempted using the user account used to start the update (see 6.4 on pg. 61).

  If the proxy server requires **authentication** and you did not enter the username and **password** or the data specified were not accepted by the proxy server for some reason, a window will pop up when updates start, asking for a username and password for authentication. If authentication is successful, the username and password will be used at next updates. Otherwise, the authentication settings will be requested again.

To avoid using a proxy when the update source is a local folder, select the **Bypass proxy server for local addresses**.

10.4.4. Update distribution

The update copying feature makes it possible to optimize the load on your business's network. Updates are copied in two stages:

1. One of the computers on the network retrieves an application and threat signature update package from the Kaspersky Lab web servers or from another web resource hosting a current set of updates. The updates retrieved are placed in a public access folder.
2. Other computers on the network access the public access folder to retrieve application updates.

To enable update distribution, select the **Update distribution folder** checkbox on the **Additional** tab (see Figure 34), and in the field below, specify the shared folder where updates retrieved will be placed. You can enter the path manually or selected in the window that opens when you click **Browse**. If the

checkbox is selected, updates will automatically be copied to this folder when they are retrieved.

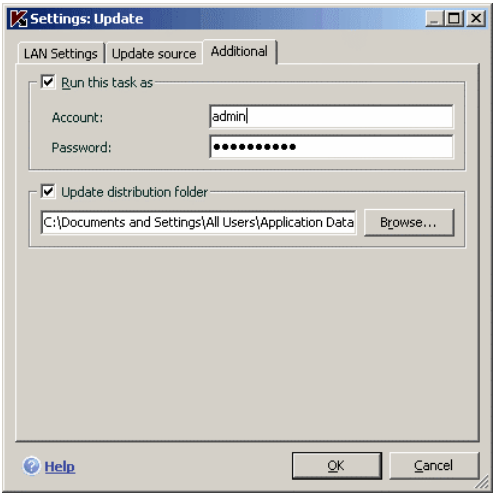


Figure 34. Copy updates tool settings

You can also specify the method for update distribution:

- *complete*, which copies threat signatures and component updates for all Kaspersky Lab 6.0 applications. To select complete updates, select the **Copy updates for all components** checkbox.
- *custom*, which only copies threat signatures and updates for the Kaspersky Anti-Virus 6.0 components that are installed. If you want to select this update method, you must deselect the **Copy updates for all components** checkbox.

If you want other computers on the network to update from the folder that contains updates copied from the Internet, you must take the following steps:

1. Grant public access to this folder.
2. Specify the shared folder as the update source on the network computers in the Updater settings.

10.4.5. Actions after updating the program

Every threat signature update contains new records that protect your computer from the latest threats.

Kaspersky Lab recommends that you scan *quarantined objects* and *startup objects* each time after the database is updated.

Why these objects should be scanned?

The quarantine area contains objects that have been flagged by the program as suspicious or possibly infected (see 11.1 on pg. 109). Using the latest version of the threat signatures, Kaspersky Anti-Virus for Windows Servers may be able to identify the threat and eliminate it.

By default, the application scans quarantined objects after each threat signature update. You are also advised to periodically view the quarantined objects because their statuses can change after several scans. Some objects can then be restored to their previous locations, and you will be able to continue working with them.

To disable scans of quarantined objects, uncheck **Rescan Quarantine** in the **Action after Update** section.

Startup objects are critical for the safety of your computer. If one of them is infected with a malicious application, this could cause an operating system startup failure. Kaspersky Anti-Virus for Windows Servers has a built-in scan task for startup objects (see Chapter 8 on pg. 79). You are advised to set up a schedule for this task so that it is launched automatically after each threat signature update (see 6.5 on pg. 62).

CHAPTER 11. ADVANCED OPTIONS

Kaspersky Anti-Virus for Windows Servers has other features that expand its functionality.

The program places some objects in special storage areas, in order to ensure maximum protection of data with minimum losses.

- Backup contains copies of objects that Kaspersky Anti-Virus for Windows Servers has changed or deleted (see 11.2 on pg. 112). If any object contained information that was important to you and could not be fully recovered during anti-virus processing, you can always restore the object from its backup copy.
- Quarantine contains potentially infected objects that could not be processed using the current threat signatures (see 11.1 on pg. 109).

It is recommended that you periodically examine the list of stored objects. Some of them may already be outdated, and some may have been restored.

The advanced options include a number of diverse useful features. For example:

- Technical Support provides comprehensive assistance with Kaspersky Anti-Virus for Windows Servers (see 11.6 on pg. 124). Kaspersky provides you with several channels for support, including on-line support and a questions and comments forum for program users.
- The Notifications feature sets up user notifications about key events for Kaspersky Anti-Virus for Windows Servers (see 11.8.1 on pg. 128). These could be either events of an informative nature, or critical errors that must be eliminated immediately.
- Self-Defense protects the program's own files from being modified or damaged by hackers, blocks remote administration from using the program's features, and restricts server administrator rights on your computer from performing certain actions in Kaspersky Anti-Virus for Windows Servers (see 11.8.2 on pg. 133). For example, changing the level of protection can significantly influence information security on your computer.
- License Key Manager can obtain detailed information on the license used, activate your copy of the program, and manage license key files (see 11.5 on pg. 123).

The program also provides a Help section (see 11.4 on pg. 122) and detailed reports (see 11.3 on pg. 114) on the operation of File Anti-Virus and virus scan and update tasks.

You can also change the appearance of Kaspersky Anti-Virus for Windows Servers and can customize the program interface (see 11.7 on pg. 126).

The following sections discuss these features in more detail.

11.1. Quarantine for potentially infected objects

Quarantine is a special storage area that holds potentially infected objects.

Potentially infected objects are objects that are suspected of being infected with viruses or modifications of them.

Why *potentially infected*? This are several reasons why it is not always possible to determine whether an object is infected:

- The code of the object scanned resembles a known threat but is partially modified.

  Threat signatures contain threats that have already been studied by Kaspersky Lab. If a malicious program is modified by a hacker but these changes have not yet been entered into the signatures, Kaspersky Anti-Virus for Windows Servers classifies the object infected with this changed malicious program as being potentially infected, and indicates what threat this infection resembles.

- The code of the object detected is reminiscent in structure of a malicious program, although nothing similar is recorded in the threat signatures.

  It is quite possible that this is a new type of threat, so Kaspersky Anti-Virus for Windows Servers classifies the object as a potentially infected object.

The *heuristic code* analyzer detects potential viruses. This mechanism is fairly effective and very rarely produces false positives.

A potentially infected object can be detected and placed in quarantine by File Anti-Virus or in the course of a virus scan.

You can place an object in quarantine by clicking **Quarantine** in the notification that pops up when a potentially infected object is detected.

When you place an object in Quarantine, it is moved, not copied. The object is deleted from the disk or email and is saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

11.1.1. Actions with quarantined objects

The total number of objects in Quarantine is displayed by selecting the **Data files** item in the **Service** area of the application's main window. In the right-hand part of the screen the *Quarantine* section displays:

- the number of potentially infected objects detected during Kaspersky Anti-Virus for Windows Servers operation;
- the current size of Quarantine.

Here you can delete all objects in the quarantine with the **Clean up** button. Note that in doing so the Backup files and report files will also be deleted.

To access objects in Quarantine:

left-click in any part of the **Quarantine** section.

You can take the following actions on the **Quarantine** tab (see Figure 35):

- Move a file to Quarantine that you suspect is infected but the program did not detect. To do so, click **Add** and select the file in the standard selection window. It will be added to the list with the status *added by user*.
- Scan and disinfect all potentially infected objects in Quarantine using the current threat signatures by clicking, click **Scan all**.

  After scanning and disinfecting any quarantined object, its status may change to *infected, potentially infected, false positive, OK,* etc.

  The *infected* status means that the object has been identified as infected but it could not be treated. You are advised to delete such objects.

  All objects marked *false positive* can be restored, since their former status as *potentially infected* was not confirmed by the program once scanned again.

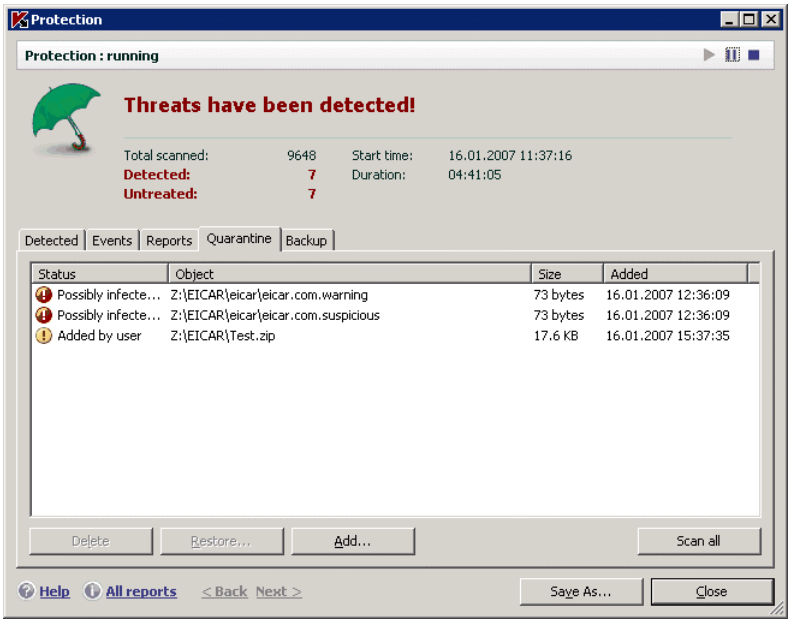


Figure 35. List of quarantined objects

- Restore the files to a selected folder or their original folder prior to Quarantine (default). To restore an object, select it from the list and click **Restore**. When restoring objects from archives, email databases, and email format files placed in Quarantine, you must also select the directory to restore them to.

> Tip:
>
> We recommend that you only restore objects with the status *false positive, OK,* and *disinfected*, since restoring other objects could lead to infecting your computer.

- Delete any quarantined object or group of selected objects. Only delete objects that cannot be disinfected. To delete the objects, select them in the list and click **Delete**.

11.1.2. Setting up Quarantine

You can configure the settings for the layout and operation of Quarantine, specifically:

- Set up automatic scans for objects in Quarantine after each threat signature update (for more details, see 10.4.4 on pg. 105).

> Warning!
>
> The program will not be able to scan quarantined objects immediately after updating the threat signatures if you are accessing the Quarantine area.

- Set the maximum Quarantine storage time.

  The default storage time 30 days, at the end of which objects are deleted. You can change the Quarantine storage time or disable this restriction altogether.

To do so:

1. Open the Kaspersky Anti-Virus for Windows Servers settings window by clicking Settings in the main program window.
2. Select **Data Files** from the settings tree.
3. In the **Quarantine & Backup** section (see Figure 36), enter the length of time after which objects in Quarantine will be automatically deleted. Alternately, uncheck the checkbox to disable automatic deletion.

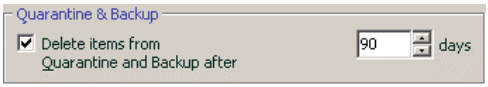


Figure 36. Configuring the Quarantine storage period

11.2. Backup copies of dangerous objects

Sometimes when objects are disinfected their integrity is lost. If a disinfected file contains important information that is partially or fully corrupted, you can attempt to restore the original object from a backup copy.

A **backup copy** is a copy of the original dangerous object that is created before the object is disinfected or deleted. It is saved in Backup.

Backup is a special storage area that contains backup copies of dangerous objects. Files in backup are saved in a special format and are not dangerous.

11.2.1. Actions with backup copies

The total number of backup copies of objects in Backup is displayed in the **Data files** in the **Service** section of the application's main window. In the right-hand part of the screen the *Backup* section displays:

- the number of backup copies of objects created by Kaspersky Anti-Virus for Windows Servers
- the current size of Backup.

Here you can delete all the copies in Backup with the **Clean up** button. Note that in doing so the Quarantine objects and report files will also be deleted.

To access dangerous object copies:

left-click in any part of the **Backup** section.

A list of backup copies is displayed in the **Backup** tab (see Figure 37). The following information is displayed for each copy: the path and filename of the object, the status of the object assigned by the scan, and its size.

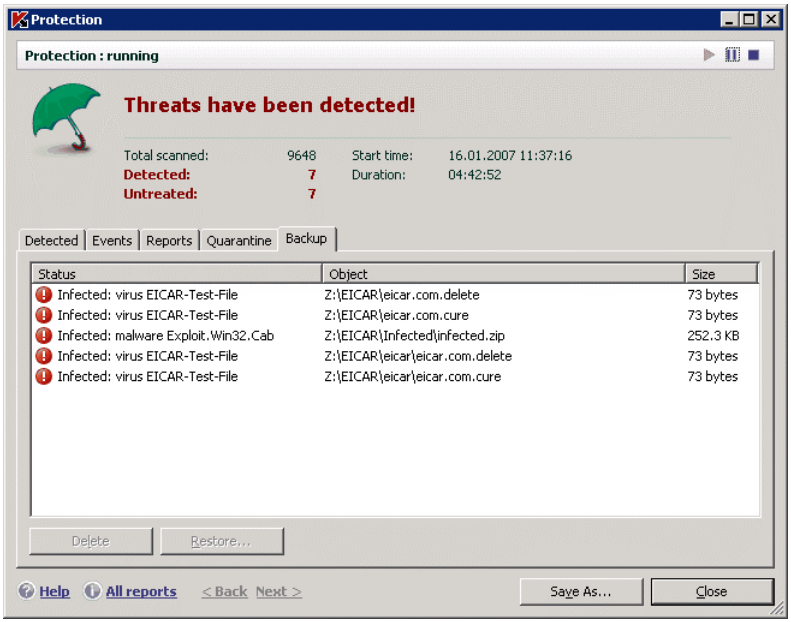


Figure 37. Backup copies of deleted or disinfected objects

You can restore selected copies using the **Restore** button. The object is restored from Backup with the same name that it had prior to disinfection.

If there is an object in the original location with that name (this is possible if a copy was made of the object being restored prior to disinfection), a warning will be given. You can change the location of the restored object or rename it.

You are advised to scan backup objects for viruses immediately after restoring them. It is possible that with updated signatures you will be able to disinfect it without losing file integrity.

You are advised **not** to restore backup copies of objects unless absolutely necessary. This could lead to an infection on your computer.

You are advised to periodically examine the Backup area, and empty it using the **Delete** button. You can also set up the program so that it automatically deletes the oldest copies from Backup (see 11.2.2 on pg. 114).

11.2.2. Configuring Backup settings

You can define the maximum time that backup copes remain in the Backup area.

The default Backup storage time is 90 days, at the end of which backup copies are deleted. You can change the storage time or remove this restriction altogether. To do so:

1. Open the Kaspersky Anti-Virus for Windows Servers settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. Set the duration for storing backup copies in the repository in the **Quarantine and Backup** section (see Figure 36) on the right-hand part of the screen. Alternately, uncheck the checkbox to disable automatic deletion.

11.3. Reports

File Anti-Virus, virus task scans and updates are all recorded in reports.

The total number of reports created by the program and their total size is displayed by clicking on **Data files** in the **Service** section of the main program window. The information is displayed in the *Reports* box.

To view reports:

Left-click anywhere in the *Reports* box to open the Protection window, which summarizes protection given by the application. The window will open to the **Reports** tab (see Figure 38).

The Reports tab lists the latest reports on File Anti-Virus, update and virus scan tasks run during the current session of Kaspersky Anti-Virus for Windows Servers. The status is listed beside File Anti-Virus or task, for example, *stopped* or *complete*. If you want to view the full history of report creation for the current session of the program, check **Show report history**.

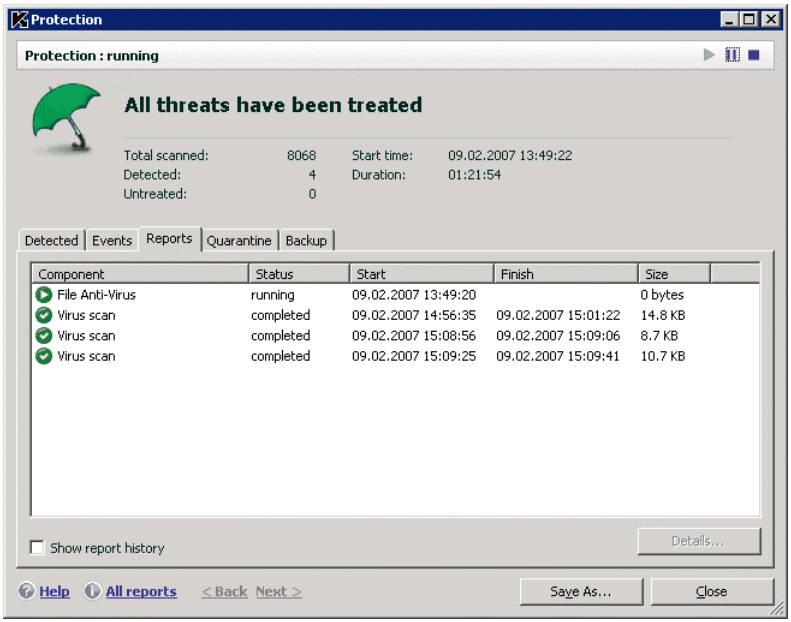


Figure 38. Reports on component operation

To review all the events reported for File Anti-Virus or task:

Select File Anti-Virus or the task on the **Reports** tab and click the **Details** button.

A window will then open that contains detailed information on the performance of File Anti-Virus or the task. The resulting performance statistics are displayed in the upper part of the window, and detailed information is provided on the tabs.

- The **Detected** tab contains a list of dangerous objects detected by File Anti-Virus or a virus scan task performed.

- The **Events** tab displays File Anti-Virus or task events.
- The **Statistics** tab contains detailed statistics for all scanned objects.
- The **Settings** tab displays settings used by File Anti-Virus, virus scans, or threat signature updates.
- The **Banned users** tab displays a list of users whose computers have been banned when attempting to copy an infected or potentially infected files to the server.

You can export the entire report as a text file. This feature is useful when an error has occurred in File Anti-Virus that you cannot eliminate on your own, and you need assistance from Technical Support. If this happens, the report must be sent as a .txt file to Technical Support to enable our specialists can study the problem in detail and solve it as soon as possible.

To export a report as a text file:

Click **Save as** and specify where you want to save the report file.

After you are done working with the report, click **Close**.

There is an Actions button on all the tabs (except **Settings** and **Statistics**) which you can use to define responses to objects on the list. When you click it, a context-sensitive menu opens with a selection of these menu items (the menu differs depending on the component – all the possible options are listed below):

Disinfect – attempts to disinfect a dangerous object. If the object is not successfully disinfected, you can leave it on this list to scan later with updated threat signatures or delete it. You can apply this action to a single object on the list or to several selected objects.

Discard – delete record on detecting the object from the report.

Add to trusted zone – exclude the object from protection. A window will open with an exclusion rule for the object.

Go to File – open the folder where the object is located in Windows Explorer.

Disinfect All – neutralize all objects on the list. Kaspersky Anti-Virus for Windows Servers will attempt to process the objects using threat signatures.

Discard All – clear the report on detected objects. When you use this function, all detected dangerous objects remain on your computer.

Search www.viruslist.com – go to a description of the object in the Virus Encyclopedia on the Kaspersky Lab website.

Search www.google.com – find information on the object using this search engine.

Search – enter search terms for objects on the list by name or status.

In addition, you can sort the information displayed in the window in ascending and descending order for each of the columns, by clicking on the column head.

Dangerous objects detected by Kaspersky Anti-Virus are processed using the **Disinfect** button (for one object or a group of selected objects) or **Disinfect all** (to process all the objects on the list). When each object is processed, a notification will be displayed on the screen, where you must decide what actions will be taken next.

If you check **Apply to all** in the notification window, the selected action will be applied to all objects with the same status selected from the list before beginning processing.

11.3.1. Configuring report settings

To configure settings for creating and saving reports:

Open the Kaspersky Anti-Virus for Windows Servers settings window by clicking Settings in the main program window.

1. Select **Data files** from the settings tree.
2. Edit the settings in the **Reports** box (see Figure 39) as follows:
   - Allow or disable logging informative events. These events are generally not important for security. To log events, check **Log non-critical events**;
   - Choose only to report events that have occurred since the last time the task was run. This saves disk space by reducing the report size. If **Keep only recent events** is checked, the report will begin from scratch every time you restart the task. However, only non-critical information will be overwritten.
   - Set the storage time for reports. By default, the report storage time is 90 days, at the end of which the reports are deleted. You can change the maximum storage time or remove this restriction altogether.

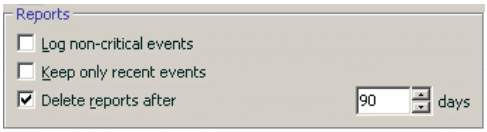


Figure 39. Configuring report settings

11.3.2. The *Detected* tab

This tab (see Figure 40) contains a list of dangerous objects detected by Kaspersky Anti-Virus for Windows Servers. The full filename and path is shown

for each object, with the status assigned to it by the program when it was scanned or processed.

If you want the list to contain both dangerous objects and successfully neutralized objects, check **Show neutralized objects**.

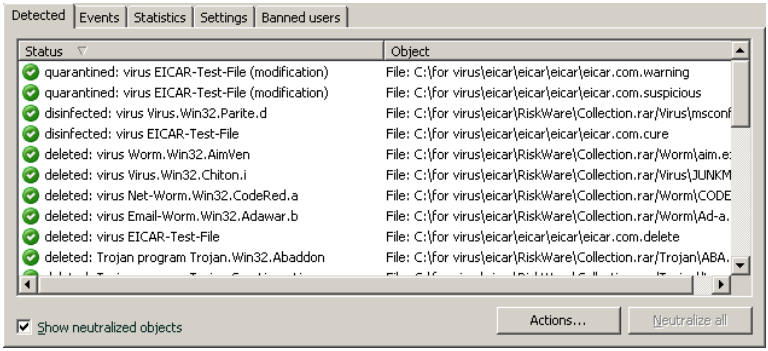


Figure 40. List of detected dangerous objects

Dangerous objects detected by Kaspersky Anti-Virus are processed using the **Neutralize** button (for one object or a group of selected objects) or **Neutralize all** (to process all the objects on the list). When each object is processed, a notification will be displayed on the screen, where you must decide what actions will be taken next.

If you check **Apply to all** in the notification window, the selected action will be applied to all objects with the same status selected from the list before beginning processing.

11.3.3. The *Events* tab

This tab (see Figure 41) provides you with a complete list of all the important events in File Anti-Virus operation, virus scans, and threat signature updates.

These events can be:

Critical events are events of a critical importance that point to problems in program operation or vulnerabilities on your computer. For example, *virus detected*, *error in operation*.

Important events are events that must be investigated, since they reflect important situations in the operation of the program. For example, *stopped.*

Informative messages are reference-type messages that generally do not contain important information. For example, *OK, not processed*. These

events are only reflected in the event log if **Show all events** is checked.

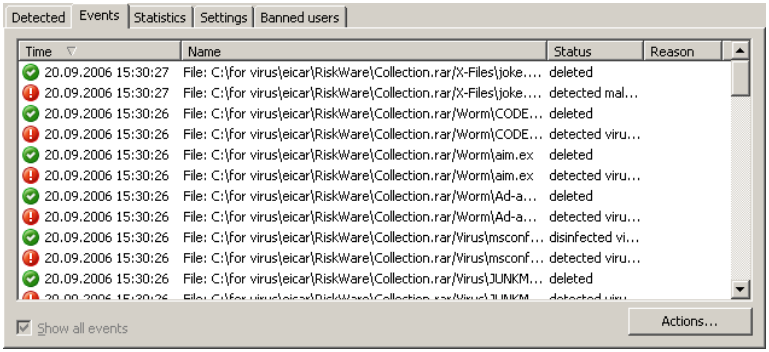


Figure 41. Events processed by the component

The format for displaying events in the event log may vary with the component or task. The following information is given for update tasks:

- Event name
- Name of the object involved in the event
- Time when the event occurred
- Size of the file loaded

For virus scan tasks, the event log contains the name of the object scanned and the status assigned to it by the scan/processing.

11.3.4. The Statistics tab

This tab (see Figure 42) provides you with detailed statistics on File Anti-Virus and virus scan tasks. Here you can learn:

- How many objects were scanned for dangerous traits in this session of File Anti-Virus, or after a task is completed. The number of scanned archives, compressed files, and password protected and corrupted objects is displayed.
- How many dangerous objects were detected, not disinfected, deleted, or placed in Quarantine.

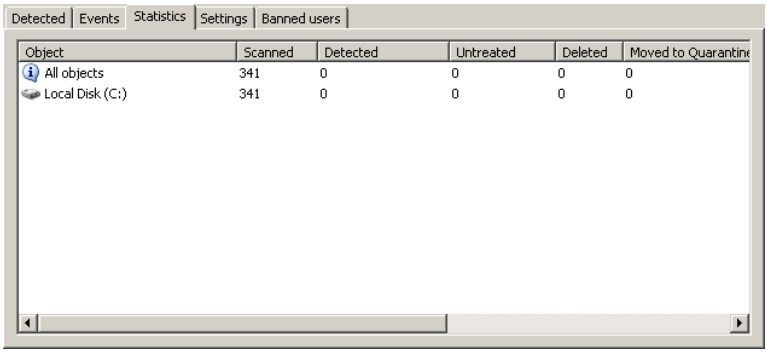


Figure 42. Component statistics

11.3.5. The Settings tab

The **Settings** tab (see Figure 43) displays a complete overview of the settings for File Anti-Virus, virus scans and program updates. You can find out the current security level for File Anti-Virus or virus scan, what actions are being taken with dangerous objects, or what settings are being used for program updates. Use the Change settings link to configure the component.

You can configure advanced settings for virus scans:

- Establish the priority of scan tasks used if the processor is heavily loaded. The ☑ **Concede resources to other applications** box is checked by default. With this feature, the program tracks the load on the processor and disk subsystems for the activity of other applications. If the load on the processor increases significantly and prevents the user's applications from operating normally, the program reduces scanning activity. This increases scan time and frees up resources for the user's applications.

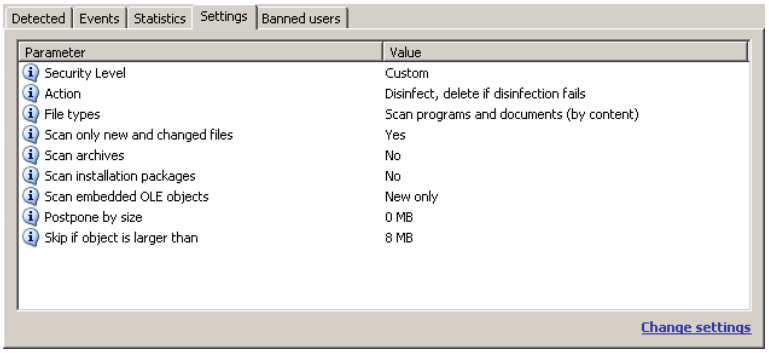


Figure 43. Component settings

- Set the computer's mode of operation for after a virus scan is complete. You can configure the computer to shut down, restart, or go into standby or sleep mode. To select an option, left-click on the hyperlink until it displays the option you need.

11.3.6. The *Banned users* tab

(see Figure 44). Every computer that has attempted to copy an infected or potentially infected file to the server is blocked. Banning a computer can additionally be applied to actions related to processing the file (disinfecting or deleting).

This tab tells you which computers have been banned, along with the date and time when this occurred, and how many hours are left until they are unbanned.

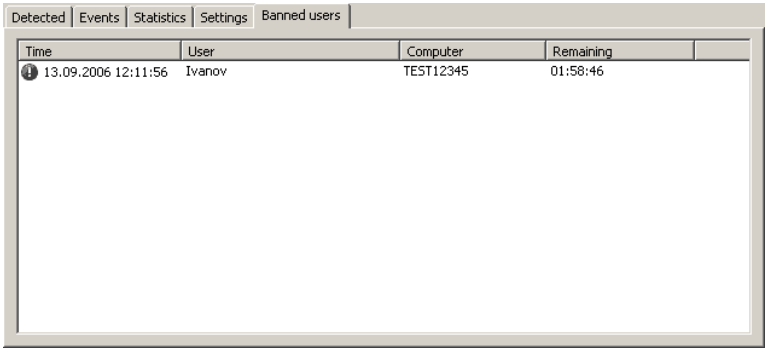


Figure 44. List of banned users

11.4. General information about the program

You can view general information on the program in the **Service** section of the main window (see Figure 45).

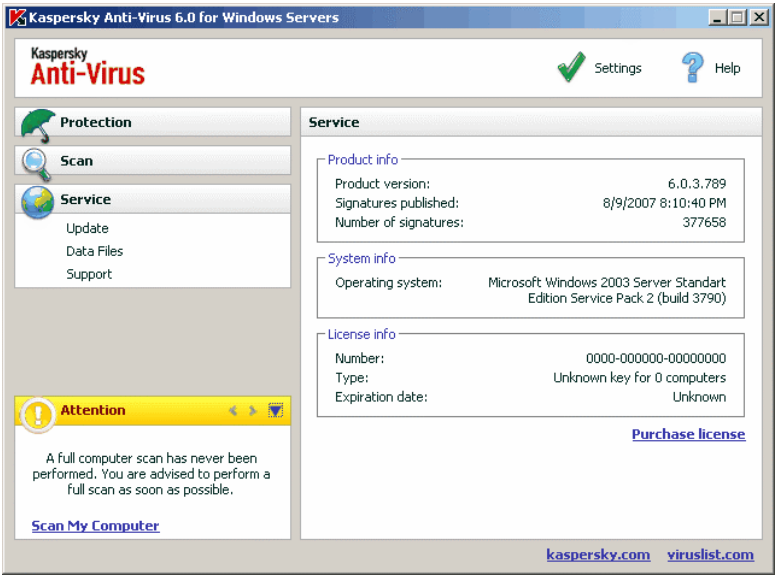


Figure 45. Information on the program, the license, and the system it is installed on

All the information is broken into three sections:

- The program version, the date of the last update, and the number of threats known to date are displayed in the **Product info** box.
- Basic information on the operation system installed on your computer is shown in the **System info** box.
- Basic information about the license you purchased for Kaspersky Anti-Virus is contained in the **License info** box.

You will need all this information when you contact Kaspersky Lab Technical Support (see 11.6 on pg. 124).

11.5. Managing licenses

Kaspersky Anti-Virus for Windows Servers needs a *license key* to operate. You are provided with a key when you buy the program. It gives you the right to use the program from the day you install the key.

Without a license key, unless a trial version of the application has been activated, Kaspersky Anti-Virus will run in one update mode. The program will not download any new updates.

If a trial version of the program has been activated, after the trial period expires, Kaspersky Anti-Virus will not run.

When the commercial license key expires, the program will continue working, except that you will not be able to update threat signatures. As before, you will be able to scan your computer for viruses and use the protection components, but only using the threat signatures that you had when the license expired. We cannot guarantee that you will be protected from viruses that surface after your program license expires.

To avoid infecting your computer with new viruses, we recommend extending your Kaspersky Anti-Virus for Windows Servers license. The program will notify you two weeks prior to the expiration of your license, and for the next two weeks it will display this message every time you open it.

To renew the license, you will need to purchase and install a new application license key or enter an application activation code. To do so:

Contact your product vendor and purchase an application license key or application code.

or:

Obtain a license key or activation code directly from Kaspersky Lab by clicking the Obtain license link in the license key window (see Figure 46). Complete the form on our website. Once payment is made, a link will be sent to the email address you entered in the order form. This link will enable you to download an application license key or obtain an activation code.

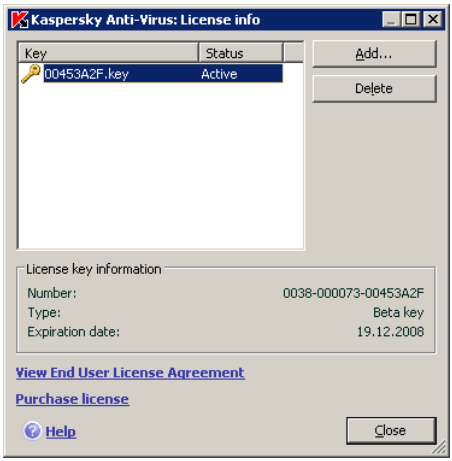


Figure 46. License information

Kaspersky Lab regularly has special pricing offers on license extensions for our products. Check for specials on the Kaspersky Lab website in the **Products → Sales and special offers** area.

Information about the license key used is available in the **License info** box in the **Service** section of the main program window. To open the license manager window, left-click anywhere in the box. In the window that opens (see Figure 46), you can view information on the current key, add a key, or delete a key.

When you select a key from the list in the **License info** box, information will be displayed on the license number, type, and expiration date. To add a new license key, click **Add** and activate the application with the activation wizard (see 11.5 on pg. (see 11.6 on pg. 124)). To delete a key from the list, use the **Delete** button.

To review the terms of the EULA, click View End User License Agreement. To purchase a license using a web form on the Kaspersky Lab website, click Purchase license.

11.6. Technical Support

Kaspersky Anti-Virus for Windows Servers provides you with a wide range of options for questions and problems related to program operation. They are all located in **Support** (see Figure 47) in the **Service** section.

Depending on the problem, we provide several technical support services:

User forum. This resource is a dedicated section of the Kaspersky Lab website with questions, comments, and suggestions by program users. You can look through the basic topics of the forum and to leave a comment yourself. You also might find the answer to your question.

To access this resource, use the User forum link.

Knowledge Base. This resource is also a dedicated section of the Kaspersky Lab website and contains Technical Support recommendations for using Kaspersky Lab software and answers to frequently asked questions. Try to find an answer to your question or a solution to your problem with this resource.

To obtain technical support online, click the Knowledge Base link.

Comments on program operation. This service is designed for posting comments on program operation or describing a problem that surfaced in program operation. You must fill out a special form on the company's website that describes the situation in detail. In order to best deal with the problem, Kaspersky Lab will need some information about the system. You can describe the system configuration on your own or use the automatic information collector on your computer.

To go to the comment form, use the Submit a bug report or a suggestion link.

Technical support. If you need help with using Kaspersky Anti-Virus, click the link located in the **Local Technical Support** box. The Kaspersky Lab website will then open with information about how to contact our specialists.

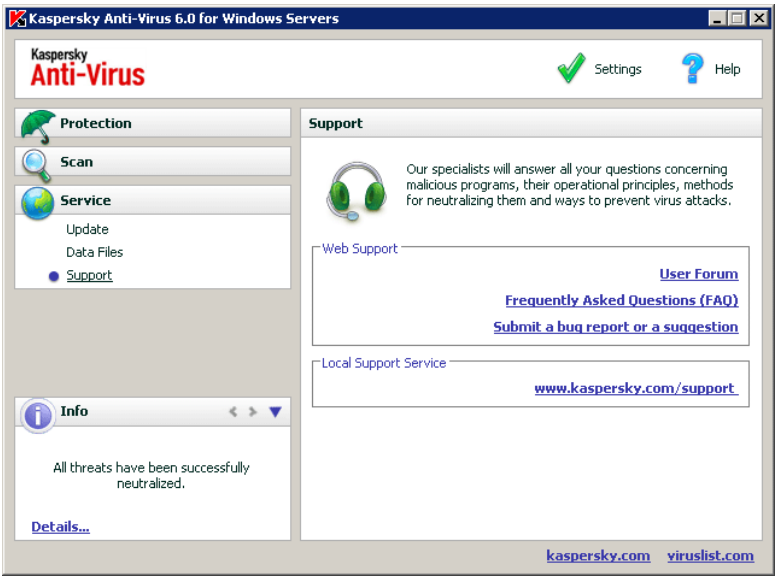


Figure 47. Technical support information

11.7. Configuring the Kaspersky Anti-Virus for Windows Servers interface

Kaspersky Anti-Virus for Windows Servers gives you the option of changing the appearance of the program by creating and using skins. You can also configure the use of active interface elements such as the system tray icon and popup messages.

To configure the program interface, take the following steps:

1. Open the Kaspersky Anti-Virus for Windows Servers settings window by clicking the Settings link in the main window.
2. Select **Appearance** in the **Service** section of the program settings tree (see Figure 48).

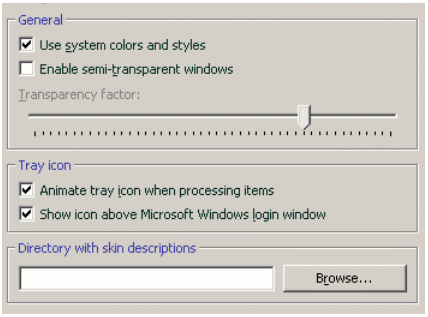


Figure 48. Configuring program appearance settings

In the right-hand part of the settings window, you can determine:

- Whether to display the Kaspersky Anti-Virus for Windows Servers protection indicator when the operating system starts.

  This indicator by default appears in the upper right-hand corner of the screen when the program loads. It informs you that your computer is protected from all threat types. If you do not want to use the protection indicator, uncheck **Show icon above Microsoft Windows login screen**.

- Whether to use animation in the system tray icon.

  Depending on the program operation performed, the system tray icon changes. By default, icon animation is enabled. If you want to turn off animation, uncheck **Animate tray icon when processing items**. Then the icon will only reflect the protection status of your computer: if protection is enabled, the icon is in color, and if protection is paused or disabled, the icon becomes gray.

- Degree of transparency of popup messages.

  All Kaspersky Anti-Virus for Windows Servers operations that must immediately reach you or require you to make a decision are presented as popup messages above the system tray icon. The message windows are transparent so as not to interfere with other operations. If you move the cursor over the message, the transparency disappears. You can change the degree of transparency of such messages. To do so, adjust the **Transparency factor** scale to the desired position. To remove message transparency, uncheck **Enable semi-transparent windows**.

- Use your own skins for the program interface.

  All the colors, fonts, icons, and texts used in the Kaspersky Anti-Virus for Windows Servers interface can be changed. You can create your own

graphics for the program or can localize it in another language. To use a skin, specify the directory with its settings in the **Directory with skin descriptions** field. Use the **Browse** button to select the directory.

By default, the system colors and styles are used in the program's skin. You can remove them by deselecting **Use system colors and styles**. Then the styles that you specify in the screen theme settings will be used.

Note that changes to Kaspersky Anti-Virus interface settings are not saved if you restore default operation settings or uninstall the program.

11.8. Using advanced options

Kaspersky Anti-Virus for Windows Servers provides you with the following advanced features:

- Notifications of certain events that occur in the program.
- Kaspersky Anti-Virus for Windows Servers Self-Defense against modules being disabled, deleted, or edited, as well as password protection for the program.
- Resolving conflicts between Kaspersky Anti-Virus and other programs.

To configure these features:

1. Open the program setup window with the Settings link in the main window.
2. Select **Service** from the settings tree.

In the right hand part of the screen you can define whether to use additional features in program operation.

11.8.1. Kaspersky Anti-Virus for Windows Servers event notifications

Different kinds of events occur in Kaspersky Anti-Virus for Windows Servers. They can be of an informative nature or contain important information. For example, an event can inform you that the program has updated successfully, or can record an error in a component that must be immediately eliminated.

To receive updates on Kaspersky Anti-Virus for Windows Servers operation, you can use the notification feature.

Notices can be delivered in several ways:

- Popup messages above the program icon in the system tray
- Sound messages
- Emails
- Log event

To use this feature, you must:

1. Check **Enable notifications** in the **Interaction with user** box (see Figure 49).

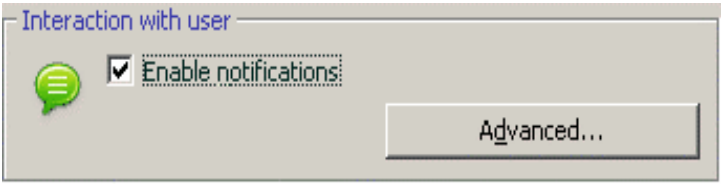


Figure 49. Enabling notifications

2. Define the event types from Kaspersky Anti-Virus for Windows Servers for which you want notifications, and the notification delivery method (see 11.8.1.1 on pg. 129).
3. Configure email notification delivery settings, if that is the notification method that is being used (see 11.8.1.2 on pg. 131).

11.8.1.1. Types of events and notification delivery methods

During Kaspersky Anti-Virus for Windows Servers operation, the following kinds of events arise:

Critical notifications are events of a critical importance. Notifications are highly recommended, since they point to problems in program operation or vulnerabilities in protection on your computer. For example, *threat signatures corrupt* or *license expired*.

Functional failure – events that lead to the application not working. For example, no license or threat signatures.

Important notifications are events that must be investigated, since they reflect important situations in the operation of the program. For example, *protection disabled* or *computer has not been scanned for viruses for a long time.*

Not important notifications are reference-type messages that generally do not contain important information. For example, *all dangerous objects disinfected*.

To specify which events the program should notify you of and how:

1. Click the Settings link in the program's main window.
2. In the program settings window, select **Service**, check ☑ **Enable notifications**, and edit detailed settings by clicking the **Settings** button.

You can configure the following notification methods for the events listed above in the **Notification settings** window that opens (see Figure 50):

- *Popup messages* above the program icon in the system tray that contain an informative message on the event that occurred.

  To use this notification type, check ☑ in the **Balloon** section across from the event about which you want to be informed.

- *Sound notification*

  If you want this notice to be accompanied by a sound, check ☑ **Sound** across from the event.

- *Email notification*

  To use this type of notice, check the ☑ **Email** column across from the event about which you want to be informed, and configure settings for sending notices (see 11.8.1.2 on pg. 131).

- *Log event*

  To record information about any event occurring in the log, check the box across from it ☑ in the **Log** chart and configure the event log settings (see 11.8.1.3 on pg. 132).

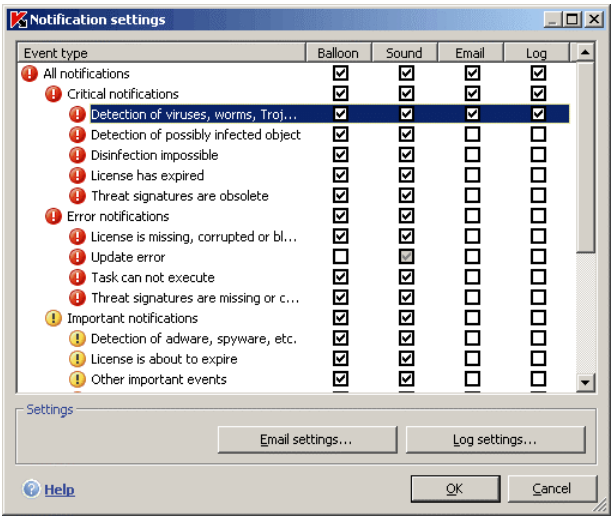


Figure 50. Program events and event notification methods

11.8.1.2. Configuring email notification

After you have selected the events (see 11.8.1.1 on pg. 129) about which you wish to receive email notifications, you must set up notification delivery. To do so:

1. Open the program setup window with the Settings link in the main window.
2. Select **Service** in the settings tree.
3. Click **Advanced** in the **Interaction with user** section of the right-hand part of the screen.
4. On the **Notification settings** tab, select the ☑ checkbox in the **Email** graph for events that should trigger an e-mail message.
5. In the window that opens when you click **Email settings**, configure the following settings for sending e-mail notifications:
    - Assign the sending notification setting for **From: Email address**.

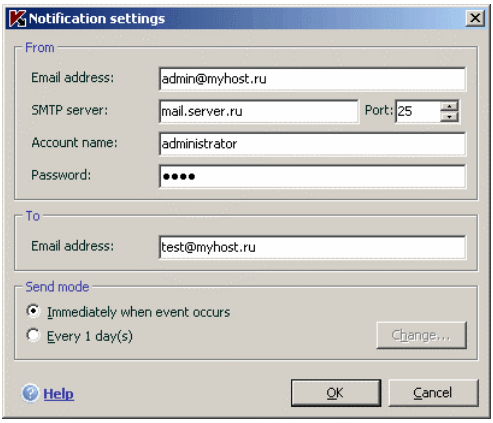


Figure 51. Configuring email notification settings

- Specify the email address to which notices will be sent in **To: Email address**.
- Assign a email notification delivery method in the **Send mode**. If you want the program to send email as soon as the event occurs, select **Immediately when event occurs**. For notifications about events within a certain period of time, fill out the schedule for sending informative emails by click **Change**. Daily notices are the default.

11.8.1.3. Configuring event log settings

To configure event log settings:

1. Open the application settings window with the Settings link in the main window.
2. Select **Service** in the settings tree.
3. Click **Advanced** in the **Interaction with user** section of the right-hand part of the screen.

In the **Notification settings** window, select the option of logging information for an event and click the **Log Settings** button.

Kaspersky Anti-Virus has the option of recording information about events that arise while the program is running, either in the MS Windows general event log (**Application**) or in a dedicated Kaspersky Anti-Virus event log (**Kaspersky Event Log**).

Logs can be viewed in the Microsoft Windows **Event Viewer**, which you can open by going to **Start → Settings → Control Panel → Administration → View Events**.

11.8.2. Self-Defense and access restriction

Kaspersky Anti-Virus for Windows Servers ensures your computer's security against malicious programs, and because of that , it can itself be the target of malicious programs that try to block it or delete it from the computer.

Moreover, several people may be using the same computer, all with varying levels of computer literacy. Leaving access to the program and its settings open could dramatically lower the security of the computer as a whole.

To ensure the stability of your computer's security system, Self-Defense, remote access defense, and password protection mechanisms have been added to the program.

To enable Self-Defense:

1. Open the program settings window with the Settings link in the main window.
2. Select **Service** from the settings tree.

Make the following configurations in the **Self defense** box (see Figure 52):

- **Enable Self-Defense**. If this box is checked, the program will protect its own files, processes in memory, and entries in the system registry from being deleted or modified.
- **Disable external service control**. If this box is checked, any remote administration program attempting to use the program will be blocked.

If any of the actions listed are attempted, a message will appear over the program icon in the system tray (unless the user has disabled notifications).

Figure 52. Configuring program defense

To password-protect the program, check **Enable password protection**. Click on the **Settings** button to open the **Password Protection** window, and enter the password and area that the access restriction will cover (see Figure 53).

Figure 53. Program password protection settings

You can block any program operations, except notifications for dangerous object detection, or prevent any of the following actions from being performed:

- Change of program performance settings
- Close Kaspersky Anti-Virus for Windows Servers
- Disable or pause protection on your computer

Each of these actions lowers the level of protection on your computer, so you must establish what people will work with the server.

Now whenever a user attempts to perform the actions on the server you selected, the program will request a password.

11.8.3. Resolving conflicts with other applications

In some cases, Kaspersky Anti-Virus may cause conflicts with other applications installed on a computer. This is because those programs have built-in self-defense mechanisms that turn on when Kaspersky Anti-Virus attempts to inspect them. These applications include the Authentica plug-in for Acrobat Reader, which verifies access to .pdf files, Oxygen Phone Manager II, and some computer games that have digital rights management tools.

To fix this problem, check **Compatibility mode for programs using self-protection methods** in the **Service** section of the application settings window. You must restart your operating system for this change to take effect.

11.9. Importing and exporting Kaspersky Anti-Virus for Windows Servers settings

Kaspersky Anti-Virus for Windows Servers allows you to import and export its own settings.

The settings are saved in a special configuration file.

To export the current program settings:

1. Open the Kaspersky Anti-Virus for Windows Servers main window.
2. Select the **Service** section and click Settings.
3. Click the **Save** button in the **Configuration manager** section.
4. Enter a name for the configuration file and select a save destination.

To import settings from a configuration file:

1. Open the Kaspersky Anti-Virus for Windows Servers main window.
2. Select the **Service** section and click Settings.
3. Click the **Load** button and select the file from which you want to import Kaspersky Anti-Virus for Windows Servers settings.

11.10. Resetting to default settings

It is always possible to return to the default program settings, which are considered the optimum and are recommended by Kaspersky Lab. This can be done using the Setup Wizard.

To reset protection settings:

1. Select the **Service** section and click Settings to go to the program configuration window.
2. Click the **Reset** button in the **Configuration manager** section.

The window that opens asks you to define which settings should be restored to their default values.

The program saves all the custom settings on the list by default (they are unchecked). If you do not need to save one of the settings, check the box next to it.

After you have finished configuring the settings, click the **Next** button (see 3.2 on pg. 26). Setup Wizard will open. Follow its instructions.

After you are finished with the Setup Wizard, the **Recommended** security level will be set for File Anti-Virus, except for the settings that you decided to keep. In addition, settings that you configured with the Setup Wizard will also be applied.

CHAPTER 12. ADMINISTERING THE PROGRAM WITH KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit is a system for centrally managing the key administrative tasks in operating a security system for a company network, based on the applications included in Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite.

Kaspersky Anti-Virus 6.0 for Windows Servers is one of the Kaspersky Lab products that can be administered through its own interface, the command line (these methods are described above in this documentation) or using Kaspersky Administration Kit (if the computer is a part of the centralized remote administration system).

Perform the following steps to manage Kaspersky Anti-Virus 6.0 for Windows Servers using the Kaspersky Administration Kit:

- Deploy *Administration Server* in the network; install Administration *Console* at the administrator's workplace (for more details, see the Administrator User Guide for implementing Kaspersky Administration Kit 6.0);
- On network file servers, deploy Kaspersky Anti-Virus 6.0 for Windows Servers and *NAgent* (included with Kaspersky Administration Kit) on the network's computers. For more about remote installation of Kaspersky Anti-Virus on network computers, see the Administrator Guide for implementing Kaspersky Administration Kit 6.0.

After upgrading the Kaspersky Lab administration plug-in through Kaspersky Administration Kit, close Administration Console.

Administration Console (see Figure 54) allows you to administer the application through Kaspersky Administration Kit. It is a standard **MMC-integrated interface** (Microsoft Management Console), and allows the administrator to perform the following functions:

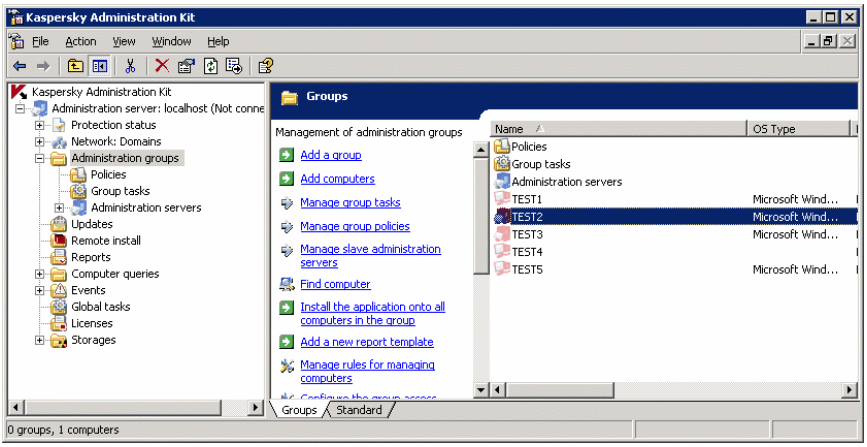


Figure 54. Kaspersky Administration Kit Administration Console

- Remotely install Kaspersky Anti-Virus 6.0 for Windows Servers and *NAgent* on network computers
- Remotely configure Kaspersky Anti-Virus on network computers
- Update Kaspersky Anti-Virus threat signatures and modules
- Manage licenses for the application on network computers
- View information about program operation on client computers

When working through Kaspersky Administration Kit, the program is administered by policy settings, task settings, and application settings set by the administrator.

Application settings are a set of settings for program operation, including general protection settings, Backup and Quarantine settings, report generation settings, etc.

Task is a specific action performed by the application. Tasks for Kaspersky Anti-Virus for Windows Servers are divided by type according to function (virus scan tasks, program update tasks, update rollback, and license key installation tasks). Each specific task has a set of Kaspersky Anti-Virus settings that are used when it is performed *(task settings)*.

The key feature of centralized administration is grouping remote computers and managing their settings by creating and configuring group policies.

A **Policy** is a group of settings for program operation on computers in network workgroups, as well as groups of restrictions on reconfiguring those settings when setting up the application or tasks on an individual client computer.

A policy includes settings for configuring all the features of the program. Thus, policies include program settings and settings for all task types, except settings specific to a certain task type.

12.1. Administering the application

Kaspersky Administration Kit gives you the opportunity to remotely start and pause Kaspersky Anti-Virus on individual client computers, as well as configuring general settings for the application, such as enabling/disabling computer protection, configuring settings for Backup and Quarantine, and configuring settings for creating reports.

To manage application settings:

1. Select the group folder that contains the client computer in the **Groups** folder (see Figure 54).
2. In the result pane, select the computer for which you need to modify application settings. In the context menu or in the **Actions** menu, select the **Properties** command.
3. The **Applications** tab on the client computer properties window (see Figure 55) displays a complete list of Kaspersky Lab applications installed on the client computer.

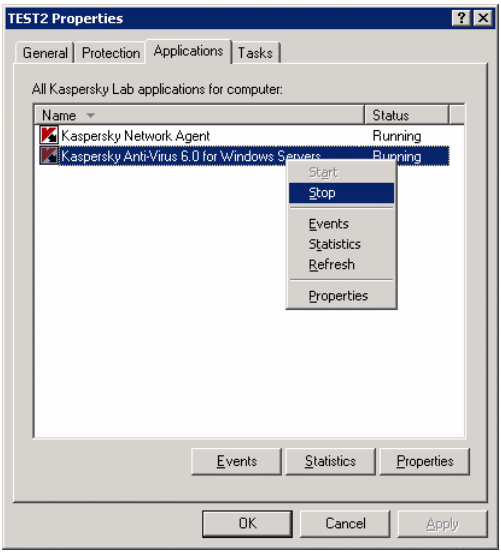


Figure 55. List of Kaspersky Lab applications

There are control buttons under the program list that you can use to:

- View a list of events in application operation that have occurred on the client and were recorded on the Administration Server
- View current statistics on program operation
- Configure program settings (see 12.1.2 on pg. 141)

12.1.1. Starting/stopping the application

You can start or pause Kaspersky Anti-Virus on a remote computer using the commands from the context menu in the computer properties window (see Figure 55).

You can execute the same actions using the **Start/Stop** buttons from the settings window on the **General** tab (see Figure 56).

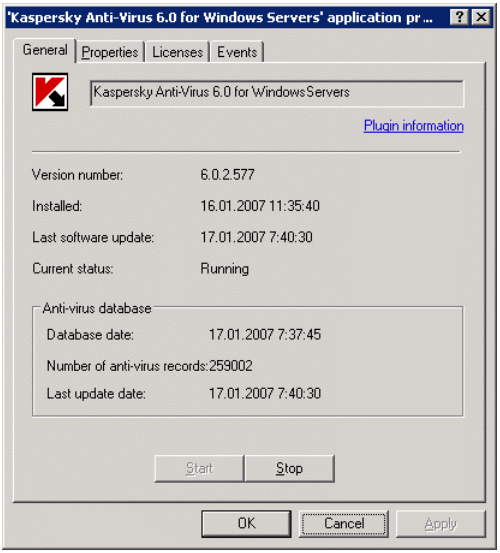


Figure 56. Configuring Kaspersky Anti-Virus settings. **General** tab

In the upper part of the window, you will find the name of the application installed, information on the version, the install date, its status (whether the application is running or paused on the local computer), and information about the threat signature database status.

12.1.2. Configuring application settings

To view or modify application settings:

1. Open the properties window for the client computer on the **Applications** tab (see Figure 54).
2. Select **Kaspersky Anti-Virus 6.0 for Windows Servers**. Click the **Properties** button to open the application settings window.

All the tabs except for the **Properties** tab are standard for Kaspersky Administration Kit. For more on the standard tabs, see the Administrator Guide.

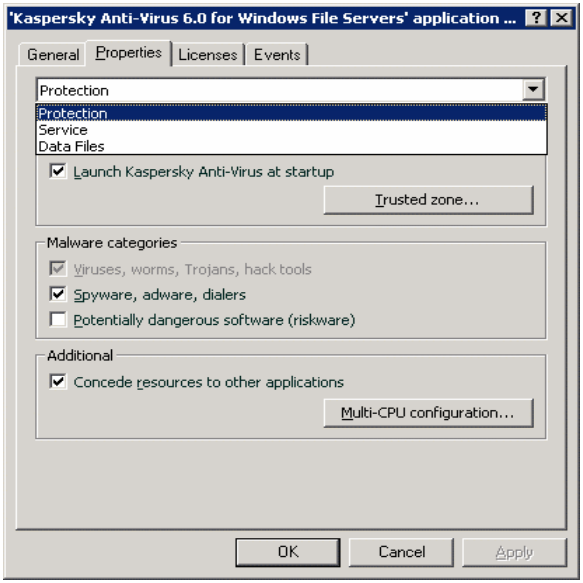


Figure 57. Configuring Kaspersky Anti-Virus settings. **Properties** tab

If a policy has been created for the application (see 12.3.1 on pg. 149) that prevents some settings from being reconfigured, they will not be editable when configuring the application.

On the **Settings** tab, you can configure general and service settings for Kaspersky Anti-Virus protection, Backup and Quarantine settings, and report creation settings. To do so, select the needed value from the dropdown menu in the upper part of the window and configure the settings:

Protection
In this window, you can: • Enable/disable protection for a computer (see 6.1 on pg. 50) • Configure automatic startup for the application when the computer is turned on (see. 6.1.5 on pg. 54) • Create a trusted zone or an exclusion list (see 6.3 on pg. 55) • Select the types of malicious programs that the application will monitor (see 6.2 on pg. 54) • Configure productivity settings for the application and multi-processor configuration settings (see 6.7 on pg. 65)
Service
Configuring service settings includes: • Configuring notifications for events that occur (see 11.8.1 on pg. 128) • Managing the application's self-defense feature and password protect application settings (see 11.8.2 on pg. 133) • Configuring the appearance of the application (see 12.3.1 on pg. 149) • Configuring settings for compatibility between Kaspersky Anti-Virus and other programs (see 11.8.3 on pg. 134)
Data Files
In this window, you can configure settings for generating report statistics on program operation (see 11.3.1 on pg. 117) and specify how long files are stored in Backup (see 11.2.2 on pg. 113) and in Quarantine (see 11.1.2 on pg. 110).

12.1.3. Configuring specific settings

When administering Kaspersky Anti-Virus through Kaspersky Administration Kit, you can enable/disable interactivity and edit information on Technical Support. To do so:

1. Open the properties window for the client computer on the **Applications** tab (see Figure 55).

2. Select **Kaspersky Anti-Virus 6.0 for Windows Servers** and use the **Properties** button. As a result, an application settings window will open (see Figure 57). Select **Service** from the dropdown menu in the upper part of the window.

On the **Service** tab of the **Appearance** section, you can enable/disable Kaspersky Anti-Virus interactivity on a remote computer: displaying the Kaspersky Anti-Virus icon in the system tray , issuing notifications on events that occur in the application (for example, detection of a dangerous object).

If **Allow interactivity** is checked, a user working on a remote computer will see the Anti-Virus icon and pop-up messages and will have the ability to make decisions on the next steps taken in notification windows regarding events that occur. To disable application interactivity, deselect the checkbox.

On the **Personal support information** tab in the window that opens when you click the **Settings** button, you can edit the information on user technical support that is displayed in the **Service** section of the **Support** item in Kaspersky Anti-Virus (see Figure 47).

To change information in the upper field, enter the current text on the support provided. In the field below, you can edit the hyperlinks that are displayed in the **Technical support online** box that is pulled up when **Support** is selected in the **Service** section.

You can edit the list of sources using the **Add**, **Edit**, and **Delete** buttons. Kaspersky Anti-Virus will add a new link to the top of the list. To change the order of the links in the list, use the **Up**/**Down** buttons.

If the window does not contain any data, the default information on technical support is not subject to editing.

12.2. Managing tasks

This section includes information on managing tasks for Kaspersky Anti-Virus 6.0 for Windows Servers. For more on the concept of managing tasks through Kaspersky Administration Kit 6.0, see the Administrator Guide for the program.

A set of system tasks is created for each computer when the application is installed. This list (see Figure 58) includes real-time protection tasks (File Anti-Virus), virus scan tasks (My Computer, Startup Objects, Critical Areas), and update tasks (threat signature and application module updates, update rollbacks, and update distribution).

You can start system tasks and configure settings and schedules for them, but they cannot be deleted.

In addition, you can create your own tasks, such as virus scans, application updates and update rollbacks, and license key installation tasks.

To view a list of the tasks created for a client computer:

1. Select the group folder that contains the client computer in the **Groups** folder (see Figure 54).
2. In the result pane, select the computer for which you need to create a local task, and use the **Tasks** command from the context menu or the same command on the **Actions** menu. Then in the main window a window will open displaying the properties of the client computer.
3. The **Tasks** tab (see Figure 58) displays a complete list of tasks created for that client computer.

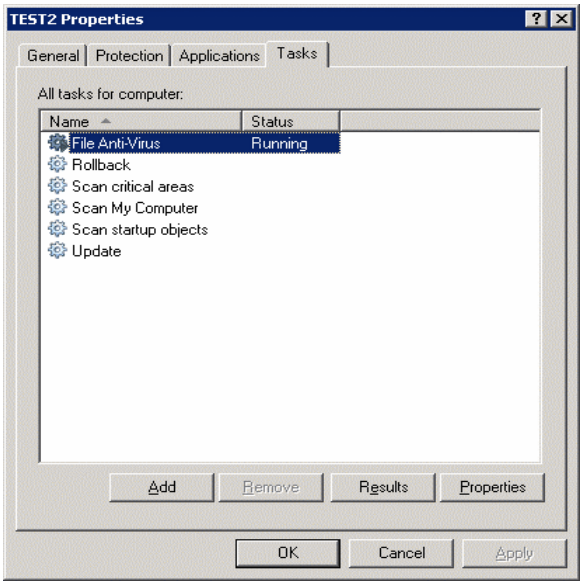


Figure 58. List of application tasks

12.2.1. Starting and stopping tasks

Tasks are started on the client computer only if the corresponding application is running (see 12.1.1 on pg. 140). If the application is stopped, all tasks started will be terminated.

Tasks are started and paused automatically, according to a schedule, or manually using commands from the context menu and from the View Task Settings window. You can also pause tasks and resume them.

To start/stop/pause/resume a task manually:

Select the necessary task from the results pane, open the context menu, and select **Start/Stop/Pause/Resume** or use the same commands on the **Action** menu.

You can start similar operations from the task settings window on the **General** tab (see Figure 59) when using the corresponding buttons.

12.2.2. Creating tasks

When working with the application through Kaspersky Administration Kit, you can create:

- Local tasks, configured for individual computers
- Group tasks, configured for computers joined in one network group
- Global tasks, configured for any set of computers from any network group

You can modify task settings, monitor their performance, copy and move tasks from one group to another, and also delete them using the standard commands **Copy/Paste**, **Cut/Paste**, and **Delete** from the context menu, or the same commands from the **Action** menu.

12.2.2.1. Creating local tasks

To create a local task, take the following steps:

1. Open the properties window for the client computer on the **Tasks** tab (see Figure 58).
2. Use the **Add** button to add a new task. This will open a Create New Task window, which is designed like a standard Windows Wizard and consists of a series of steps that you can navigate between using the **Back** and **Next** buttons or complete using the **Finished** button. The **Cancel** button will stop the process at any point.

Step 1. Entering general data on the task

The first master window is introductory: here you must specify the name of the task (the **Name** field).

Step 2. Selecting an application and task type

In this step, you must specify the application for which the task is being created (Kaspersky Anti-Virus 6.0 for Windows Servers). You must also select the task type. The possible tasks for Kaspersky Anti-Virus 6.0 are:

- *Virus scan* – scans for viruses in the areas specified by the user
- *Update* – retrieves and applies update packs for the program
- *Update Rollback* – rolls back to the last program update made
- *License key install* – adds a new license key for using the application

Step 3. Configuring settings for the selected task type

Depending on the task type selected in the previous step, the contents of the following windows can vary:

VIRUS SCAN

The virus scan task configuration window requires you to create a list of objects to be scanned (see 8.2 on pg. 80) and to specify the action Kaspersky Anti-Virus is to take when it detects a dangerous object (see 8.4.4 on pg. 87).

UPDATE

For threat signature and application module update tasks, you must specify the source that will be used to download updates (see 10.4.1 on pg. 99). The default update source is the Kaspersky Administration Kit update server.

UPDATE ROLLBACK

There are no specific settings for rolling back the most recent update.

INSTALL LICENSE KEY

For license key installation tasks, specify the path to the key file with the **Browse** button. To make an added key a backup, check ☑ **Add as backup key**. The backup license key will become active when the current license key expires.

Information about the key added (license number, type, and expiration date) is displayed in the field below.

Step 4. Configuring task start under a different user account

In this step, you are asked to configure tasks to start under a user account with sufficient privileges to access the object being scanned or update source (see 6.4 on pg. 61).

Step 5. Setting up a schedule

After configuring task settings, you will be asked to configure an automatic task schedule.

To do so, select the frequency for running the task from the dropdown menu and adjust the schedule settings in the lower part of the window.

Step 6. Finishing creating a task

The last window of the wizard will inform you that you have successfully creating a task.

12.2.2.2. Creating group tasks

To create a group task, take the following steps:

1. Select the group for which you want to create a task from the console tree.
2. Select its **Group Tasks** folder, open the context menu, and select the **Create→Task** command, or use the same command on the **Action** menu. The task creation wizard will then start, similar to the local task create wizard (for more, see 12.2.2.1 on pg. 145). Follow its instructions.

When the wizard is finished, the task will be added to the **Group Tasks** folder of that group and all the groups under it, and it will be visible in the results pane.

12.2.2.3. Creating global tasks

To create a global task, take the following steps:

1. Select the **Global tasks** node from the console tree, open the context menu, and select the **Create→Task** command, or use the same command on the **Action** menu.
2. The task creation wizard will then start, similar to the local task create wizard (for more, see 12.2.2.1 on pg. 145). The exception is that there is a stage for creating a list of client computers from the network for which the global task is being created.
3. Select from the network the computers that will run the task. You can select computers from multiple folders or select an entire folder (for more details, see the Administrator Guide for Kaspersky Administration Kit 6.0).

Global tasks are only performed on a selected set of computers. If new client computers are added to a group with computers for which a remote installation task has been created, this task will not run for them. You must create a new task or make corresponding changes to the settings of the existing task.

When the wizard is finished, a global task will be added to the **Global tasks** node of the console tree and will be visible in the results pane.

12.2.3. Configuring task settings

To view and modify client computer task settings:

1. Open the properties window for the client computer on the **Tasks** tab (see Figure 58).
2. Select the task from the list and click the **Properties** button. As a result, a task settings window will open (see Figure 60).

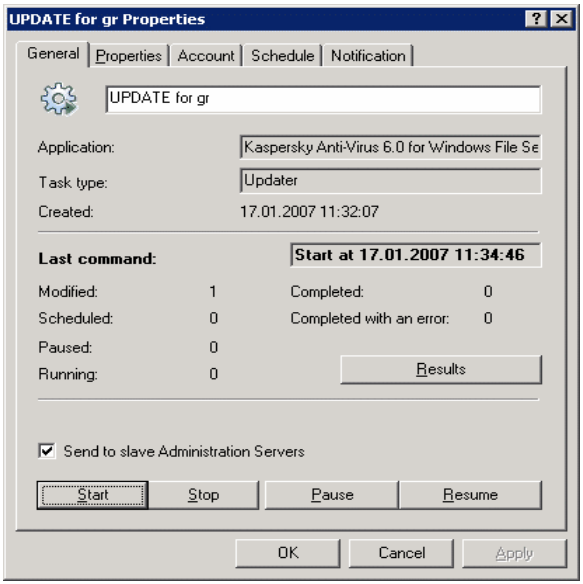


Figure 59. Configuring task settings

All the tabs except for the **Settings** tab are standard for Kaspersky Administration Kit 6.0. They are covered in greater depth in the Administrator User Guide. The **Settings** tab contains specific settings for Kaspersky Anti-Virus. The contents of this tab vary depending on the task type selected.

Configuration of program task settings through the Kaspersky Administration Kit interface is similar to configuration through the local Kaspersky Anti-Virus interface, with the exception of the settings that are specific to that task. See Chapter 7 – Chapter 10 on pp. 66 – 96 of this User Guide for a more in-depth description of configuration of task settings.

If a policy has been created for the application (see 12.3 on pg. 149) that blocks some settings from being reconfigured, they will not be editable when configuring tasks.

12.3. Managing policies

Setting up policies allows you to apply universal application and task settings to client computers that belong to a single network group.

This section includes information on creating and configuring policies for Kaspersky Anti-Virus 6.0 for Windows Servers. For more on the concept of managing policies through Kaspersky Administration Kit 6.0, see the Administrator Guide for the program.

12.3.1. Creating policies

To create a policy for Kaspersky Anti-Virus, take the following steps:

1. In the **Groups** folder (see Figure 54), select the group of computers for which you need to create a policy.
2. Select **Policies** folder that belongs to the selected group, open the context menu, and use the **Create→Policy** command. A Create New Policy window will appear.

   The Create Policy window is designed like a standard Microsoft Windows Wizard and consists of a series of steps that you can navigate between using the **Back** and **Next** buttons or complete using the **Finished** button. The **Cancel** button will stop the Wizard at any point.

During each step of creating a policy, the settings entered can be locked with the button. If the lock on the button is closed, in the future the values assigned by the policy created will be used when you use the policy on client computers.

Step 1. Entering general data on the policy

The first wizard windows are introductory. Here you must specify the name of the policy (**Name** field), select **Kaspersky Anti-Virus 6.0 for Windows Servers**

from the **Application name** dropdown menu. If you want the policy settings to take effect immediately after creating it, check **Make policy active**.

Step 2. Selecting a policy status

This window will ask you to specify the policy status. To do so, move the switch to the needed position: active policy or inactive policy.

Several policies may be created in a group for one application, but only one of them can be the current (active) policy.

Step 3. Selecting and configuring protection components

In this stage, you can enable/disable computer protection and File Anti-Virus. Protection is enable and File Anti-Virus is running by default.

To fine-tune protection settings or to configure File Anti-Virus, select it from the list and click the **Settings** button.

Step 4. Configuring virus scan tasks

In this stage, you are asked to configure the settings that will be used for virus scan tasks.

In the **Security level** box, select one of the three preset security levels (see 7.1 on pg. 67). To fine-tune the level selected, click the **Settings** button. To restore the **Recommended** protection level settings, use the **Default** button.

In the **Action** section, specify the action that Anti-Virus should take when a dangerous object is detected (see 8.4.4 on pg. 87).

Step 5. Configuring update settings

In this window, configure settings for the Kaspersky Anti-Virus update distribution feature.

In the **Update settings** section, specify whether program modules need to be updated (see 10.4.2 on pg. 100). In the window that opens when you click the **Settings** button, assign local network settings (see 10.4.3 on pg. 104) and specify the update source (see 10.4.1 on pg. 99).

In the **Actions after updating** section, enable/disable scanning of Quarantine after receiving a new update pack (see 10.4.4 on pg. 105).

Step 6. Policy enforcement

In this stage, you are asked to select a method for distributing the policy to clients in the group (for more details, consult the Kaspersky Administration Kit 6.0 Administrator Guide).

Step 7. Determining a method for first-time policy enforcement

At this step, select a method for first-time policy enforcement for client computers of the group in the **Enforce policy** window (for more details, see the Administrator Guide for Kaspersky Administration Kit 6.0).

Step 8. Finishing creating a policy

The final window of the wizard tells you that you have successfully created a policy.

Once the wizard is completed, the Kaspersky Anti-Virus policy will be added to the **Policies** folder for the corresponding group and will be visible in the results pane.

You can edit the settings of the policy created and set restrictions on modifying its settings using the button for each settings group. A user on the client computer will not be able to change settings if they are locked this way. The policy will be applied to client computers the first time the clients synchronize with the server.

You can copy or move policies from one group to another and to delete them using the standard commands **Copy**/**Paste**, **Cut**/**Paste**, and **Delete** from the context menu and the same commands from the Action menu.

12.3.2. Viewing and editing policy settings

At the editing stage, you can modify the policy and block modification to settings in nested group policies and in application and task settings.

To view and edit policy settings:

1. Select the computer group for which settings must be edited from the console tree in the **Groups** folder.
2. Select the **Policies** folder that belongs to that group. When you do so, the results pane will display all the policies created for the group.

3. Select the policy you need from the list of policies for **Kaspersky Anti-Virus 6.0 for Windows Servers** (the application name is specified in the **Application** field).

4. Open the context menu for the policy selected and click the **Properties** command. The screen will display the policy settings window for Kaspersky Anti-Virus 6.0 (see Figure 60).

All the tabs except for the **Settings** tab are standard Kaspersky Administration Kit 6.0. They are covered in greater depth in the Administrator User Guide.

The **Settings** tab displays the policy settings for Kaspersky Anti-Virus 6.0. The policy settings include program settings (see 12.1.2 on pg. 141) and task settings (see 12.2 on pg. 143).

To configure settings, select the needed value from the dropdown menu in the in the upper part of the window and configure the settings.

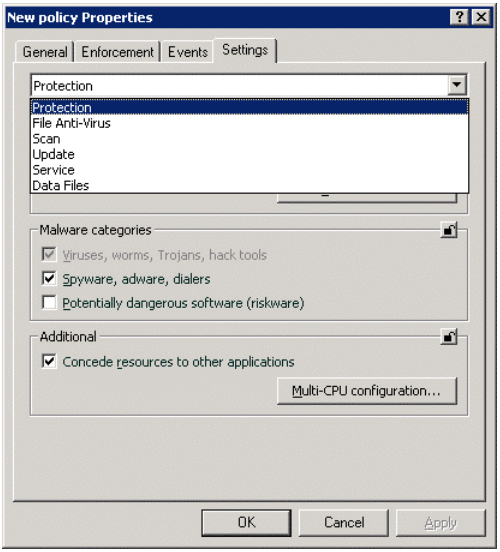


Figure 60. Configuring policy settings

CHAPTER 13. WORKING WITH THE PROGRAM FROM THE COMMAND PROMPT

You can use Kaspersky Anti-Virus for Windows Servers from the command prompt. You can execute the following operations:

- Starting, stopping, pausing and resuming the activity of File Anti-Virus
- Starting, stopping, pausing and resuming virus scans
- Obtaining information on the current status of File Anti-Virus, tasks and statistics on them
- Scanning selected objects
- Updating threat signatures and program modules
- Accessing Help for command prompt syntax
- Accessing Help for command syntax

The command prompt syntax is:

```
avp.com <command> [settings]
```

> You must access the program from the command prompt from the program installation folder or by specifying the full path to avp.com.

The following may be used as **<commands>**:

ADDKEY	Activates application using a license key file (command can only be executed if the password assigned through the program interface is entered)
ACTIVATE	Activates the application online using an activation code
START	Starts File Anti-Virus or a task
PAUSE	Pauses File Anti-Virus or a task (command can only be executed if the password assigned through the program interface is entered)

RESUME	Resumes File Anti-Virus or a task
STOP	Stops File Anti-Virus or a task (command can only be executed if the password assigned through the program interface is entered)
STATUS	Displays status of File Anti-Virus or task on screen
STATISTICS	Displays statistics for File Anti-Virus or the task on screen
HELP	Help with command syntax and the list of commands
SCAN	Scans objects for viruses
UPDATE	Begins program update
ROLLBACK	Rolls back to the last program update made (command can only be executed if the password assigned through the program interface is entered)
EXIT	Closes the program (you can only execute this command with the password assigned in the program interface)
IMPORT	Import Kaspersky Anti-Virus for Windows Servers settings (command can only be executed if the password assigned through the program interface is entered)
EXPORT	Export Kaspersky Anti-Virus for Windows Servers settings

Each command uses its own settings specific to that particular Kaspersky Anti-Virus for Windows Servers component.

13.1. Activating the application

There are two ways to activate the application:

- online using an activation code (ACTIVATE command)
- using a license key file (ADDKEY command).

Command syntax:

```
ACTIVATE <activation_code>
ADDKEY <file_name> /password=<your_password>
```

Parameters:

<file_name>	application key file name with the *.key extension.
<activation_code>	Application activation code provided at purchase.
<your_password>	Kaspersky Anti-Virus password set through the program interface.
Note that this command will not be accepted without a password.	

Example:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

13.2. Managing File Anti-Virus and tasks

Command syntax:

```
avp.com <command> <profile|task_name>
[/R[A]:<log_file>]
avp.com STOP|PAUSE <profile|task_name>
/password=<your_password> [/R[A]:<report_file>]
```

Parameters:

<command>	Kaspersky Anti-Virus provides task and component management from the command line using the commands below: **START** – start real-time security component or task. **STOP** – stop real-time security component or task. **PAUSE** – pause real-time security component or task.

	RESUME – resume real-time security component or task. **STATUS** – display current real-time security component or task status. **STATISTICS** – display current real-time security component or task runtime statistics. Please note that PAUSE and STOP are password protected.
<profile|task_name>	The **<profile>** parameter may be assigned any real-time application security component or component module, on-demand scan task, or update as value (standard values used by the application are shown below). Valid values for the **<task_name>** parameter may include the name of any user-defined on-demand scan task or update.
<your_password>	Kaspersky Anti-Virus password set through the program interface.
/R[A]:<report_file>	**R:<report_file>**: log important events only. **/RA:<report_file>**: log all events. An absolute or a relative path to a file may be used. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

One of the following values is assigned to **<profile>**:

RTP	All protection components The command `avp.com START RTP` starts File Anti-Virus if it was paused using the ⏸ button in the graphic user interface or with the PAUSE command from the command prompt. If the component was disabled using the ■ button in the graphic user interface or the STOP command from the command prompt, you must execute the command `avp.com START FM` in order for it to start.
FM	File Anti-Virus
UPDATER	Updater
RetranslationCfg	Update distribution to a local update source
Rollback	Rolls back the last update of the program
SCAN_OBJECTS	Virus scan task
SCAN_MY_COMPUTER	My Computer task
SCAN_CRITICAL_AREAS	Critical Areas task
SCAN_STARTUP	Startup Objects task
SCAN_QUARANTINE	Task for scanning Quarantined objects
Components and tasks started from the command prompt are run with the settings configured with the program interface.	

Examples:

To enable File Anti-Virus, type this at the command prompt*:*

```
avp.com START FM
```

To stop a My Computer scan task from the command prompt, enter*:*

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

13.3. Anti-virus scans

The syntax for starting a virus scan of a certain area, and processing malicious objects, from the command prompt generally looks as follows:

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>]
[<report settings>] [<advanced settings>]
```

To scan objects, you can also start one of the tasks created in Kaspersky Anti-Virus for Windows Servers from the command prompt (see 13.2 on pg. 155). The task will be run with the settings specified in the program interface.

Parameter description:

<object scanned> - this parameter gives the list of objects that will be scanned for malicious code. It can include several values from the following list, separated by spaces.	
<files>	List of paths to the files and/or folders to be scanned. You can enter absolute or relative paths. Items in the list are separated by a space. Notes: If the object name contains a space, it must be placed in quotation marks If you select a specific folder, all the files in it are scanned.
/MEMORY	System memory objects
/STARTUP	Startup objects
/MAIL	Email databases
/REMDRIVES	All removable media drives
/FIXDRIVES	All internal drives
/NETDRIVES	All network drives

/QUARANTINE	Quarantined objects
/ALL	Complete scan
/@:<filelist.lst>	Path to a file containing a list of objects and folders to be included in the scan. The file should be in a text format and each scan object must start a new line. You can enter an absolute or relative path to the file. The path must be placed in quotation marks if it contains a space.
<action> - this parameter sets responses to malicious objects detected during the scan. If this parameter is not defined, the default value is **/i8**.	
/i0	take no action on the object; simply record information about it in the report.
/i1	Treat infected objects, and if disinfection fails, skip
/i2	Treat infected objects, and if disinfection fails, delete. Exceptions: do not delete infected objects from compound objects; delete compound objects with executable headers, i.e. sfx archives (default).
/i3	Treat infected objects, and if disinfection fails, delete. Also delete all compound objects completely if infected contents cannot be deleted.
/i4	Delete infected objects, and if disinfection fails, delete. Also delete all compound objects completely if infected contents cannot be deleted.
/i8	Prompt the user for action if an infected object is detected.
/i9	Prompt the user for action at the end of the scan.
<file types> - this parameter defines the file types that will be subject to the anti-virus scan. If this parameter is not defined, the default value is /fi.	
/fe	Scan only potentially infected files by extension

/fi	Scan only potentially infected files by contents (default)
/fa	Scan all files
<exclusions> - this parameter defines objects that are excluded from the scan. It can include several values from the list provided, separated by spaces.	
-e:a	Do not scan archives
-e:b	Do not scan email databases
-e: m	Do not scan plain text emails
-e:<filemask>	Do not scan objects by mask
-e:<seconds>	Skip objects that are scanned for longer that the time specified in the **<seconds>** parameter.
-es:<size>	Skip files larger (in MB) than the value assigned by **<size>**.
<configuration file> - defines the path to the configuration file that contains the program settings for the scan. The configuration file is saved in binary format (*.dat*), unless another format is specified or if the format is not assigned, and it can be used later to import application settings on other computers. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the Kaspersky Anti-Virus for Windows Servers interface are used.	
/C:<file_name>	Use the settings values assigned in the configuration file **<file_name>**
<report settings> - this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.	

/R:<report_file>	Only log important events in this file
/RA:<report_file>	Log all events in this file
<advanced settings> – settings that define use of anti-virus scanning technologies.	
/iChecker=<on|off>	Enable/ disable iChecker.
/iSwift=<on|off>	Enable/ disable iSwift.

Examples:

*Start a scan of RAM, Startup programs, email databases, the directories **My Documents** and **Program Files**, and the file **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Pause scan of selected objects and start full computer scan, then continue to scan for viruses within the selected objects:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Scan RAM and the objects listed in the file **object2scan.txt**. Use the configuration file **scan_setting.txt**. After the scan, generate a report in which all events are recorded:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

13.4. Program updates

The syntax for updating Kaspersky Anti-Virus for Windows Servers program modules and threat signatures from the command prompt is as follows:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>]
[/C:<file_name>] [/APP=<on|off>]
```

Parameter description:

<update_source>	HTTP or FTP server or network directory for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If no path is specified, an update source will be copied from the application's update settings.
/R[A]:<report_file>	**/R:<report_file>** – only log important events in the report. **/R[A]:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.
/C:<file_name>	Path to the configuration file with the settings for program updates. The configuration file is a text file that contains a group of command prompt settings for updating the program. You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the Kaspersky Anti-Virus for Windows Servers interface are used.
/APP=<on|off>	Enable / Disable application module updates

Examples:

Update threat signatures and record all events in the report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update the Kaspersky Anti-Virus for Windows Servers program modules by using the settings in the configuration file **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Sample configuration file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

13.5. Rollback settings

Command syntax:

```
ROLLBACK
[/R[A]:<report_file>][/password=<your_password>]
```

/R[A]:<report_file>	**/R:<report_file>** – only log important events in the report. **/R[A]:<report_file>** – log all events in the report. You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.
<your_password>	Password for accessing Kaspersky Anti-Virus assigned in the application interface.
Note that you cannot execute this command without entering the password.	

Examples:

```
avp.com ROLLBACK /RA:rollback.txt
[/password=<password>]
```

13.6. Exporting settings

Command syntax:

```
avp.com EXPORT <profile> <file_name>
```

Parameter description:

<profile>	File Anti-Virus or task with the settings being exported. You can use any value for **<profile>** that is listed in 13.2 on pg. 155.

<file_name>	Path to the file to which the Kaspersky Anti-Virus for Windows Servers settings are exported. You can use an absolute or relative path. The configuration file is saved in binary format (*.dat*), unless another format is specified or if the format is not assigned, and it can be used later to import application settings on other computers. The configuration file can be saved as a text file. To do so, specify the *.txt* extension in the file name. Note that protection settings cannot be imported from a text file. This file can only be used to specify the main settings for program operation.

Examples:

```
avp.com EXPORT c:\settings.dat
```

13.7. Importing settings

Command syntax:

```
avp.com IMPORT <file_name>
[/password=<your_password>]
```

<file_name>	Path to the file from which the Kaspersky Anti-Virus for Windows Servers settings are being imported. You can use an absolute or relative path. Settings can only be imported from binary files. If you install the program in hidden mode from the command prompt or with Group Policy Object Editor, the name on the configuration file must be *install.cfg*. Otherwise the program will not recognize it.
<your_password>	Kaspersky Anti-Virus password assigned in the program interface.
Note that this command will not be accepted without a password.	

Examples:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

13.8. Starting the program

Command syntax:

```
avp.com
```

13.9. Stopping the program

Command syntax:

```
EXIT /password=<password>
```

<password>	Kaspersky Anti-Virus password assigned in the program interface.
Note that this command will not be accepted without a password.	

Note that you cannot execute this command without entering the password.

13.10. Obtaining a Trace File

A trace file may be required in the event of application runtime issues for Technical Support specialists to perform more focused troubleshooting.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

[on|off]	Enable/Disable trace file generation.
[file]	Obtain a trace and save to file.
<trace_level>	This parameter may be assigned numeric values ranging from 0 (lowest level, critical events only) to 700 (highest level, all events). When a request is sent to Technical Support, a specialist must specify the required trace level. If not specified, the recommended level is 500.

Caution! Trace file generation should be enabled to troubleshoot a specific issue only. Keeping the trace functionality active at all times may reduce computer performance and cause the hard drive to become full.

Examples:

Disable trace:

```
avp.com TRACE file off
```

Generate a trace file for Technical Support at maximum trace level of 500:

avp.com TRACE file on 500

13.11. Viewing Help

This command is available for viewing Help on command prompt syntax:

```
avp.com [ /? | HELP ]
```

To get help on the syntax of a specific command, you can use one of the following commands:

```
avp.com <command> /?
avp.com HELP <command>
```

13.12. Return codes from the command line interface

This section contains a list of return codes from the command line. The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a specific type of task.

General return codes	
0	Operation completed successfully
1	Invalid setting value
2	Unknown error
3	Task completion error

4	Task canceled
Anti-virus scan task return codes	
101	All dangerous objects processed
102	Dangerous objects detected

CHAPTER 14. MODIFYING, REPAIRING, AND REMOVING THE PROGRAM

You can uninstall the application in the following ways:

- using the application's Setup Wizard (see 14.2 on pg. 170);
- from the command prompt (see 14.2 on pg. 170);
- Using Kaspersky Administration Kit (see Kaspersky Administration Kit Implementation Guide);
- Using Microsoft Windows Server 2000/2003 group domain policies (see 3.4.3 on pg. 33).

14.1. Modifying, repairing, and removing the program using Installation Wizard

You may find it necessary to repair the program if you detect errors in its operation after incorrect configuration or file corruption.

To repair or modify Kaspersky Anti-Virus for Windows Servers missing components or delete the program:

1. Insert the installation CD into the CD-ROM drive, if you used one to install the program. If you installed Kaspersky Anti-Virus for Windows Servers from a different source (public access folder, folder on the hard drive, etc.), make sure that the installer package is in the specified source and that you have access to it.
2. Select **Start → Programs → Kaspersky Anti-Virus 6.0 for Windows Servers → Modify, Repair, or Remove**.

An installation wizard then will open for the program. Let's take a closer took at the steps of repairing, modifying, or deleting the program.

Step 1. Installation Welcome window

If you take all the steps described above necessary to repair or modify the program, the Kaspersky Anti-Virus for Windows Servers installation welcome window will appear. To continue, click the **Next** button.

Step 2. Selecting an operation

At this stage, you select which operation you want to run. You can modify the program components, repair the installed components, remove components or remove the entire program. To execute the operation you need, click the appropriate button. The program's response depends on the operation you select.

Modifying the program is like custom program installation where you can specify which components you want to install (see Step 7 on pg. 24), and which you want to delete.

Repairing the program depends on the program components installed. The files will be repaired for all components that are installed and the Recommended security level will be set for each of them.

Warning!

If Kaspersky Anti-Virus 6.0 is uninstalled remotely, the server will not restart automatically. However, to fully remove the application's components and for the computer to operate properly in the future, we recommend restarting manually.

If you remove the program, you can select which data created and used by the program you want to save on your computer. To delete all Kaspersky Anti-Virus for Windows Servers data, select **Complete uninstall**. To save data, select **Save application objects** and specify which objects not to delete from this list:

- *Activation data* – information about program activation.
- *Threat signatures* – complete set of signatures of dangerous programs, virus, and other threats current as of the last update.
- *Backup files* – backup copies of deleted or disinfected objects. You are advised to save these, in case they can be restored later.
- *Quarantine files* – files that are potentially infected by viruses or modifications of them. These files contain code that is similar to code of a known virus but it is difficult to determine if they are malicious. You are advised to save them, since they could actually not be infected, or they could be disinfected after the threat signatures are updated.
- *Application settings* – configurations for File Anti-Virus.

- *iSwift data* – database with information on objects scanned on NTFS file systems, which can increase scan speed. When it uses this database, Kaspersky Anti-Virus for Windows Servers only scans the files that have been modified since the last scan.

> Warning!
>
> If a long period of time elapses between uninstalling one version of Kaspersky Anti-Virus for Windows Servers and installing another, you are advised not to use the *iSwift* database from a previous installation. A dangerous program could penetrate the computer during this period and its effects would not be detected by the database, which could lead to an infection.

To start the operation selected, click the **Next** button. The program will begin copying the necessary files to your computer or deleting the selected components and data.

Step 3. Completing program modification, repair, or removal

The modification, repair, or removal process will be displayed on screen, after which you will be informed of its completion.

Removing the program generally requires you to restart your computer, since this is necessary to account for modifications to your system. The program will ask if you want to restart your computer. Click **Yes** to restart right away. To restart your computer later, click **No**.

14.2. Uninstalling the program from the command prompt

To uninstall Kaspersky Anti-Virus 6.0 for Windows Servers from the command prompt, enter:

```
msiexec /x <package_name>
```

The Setup Wizard will open. You can use it to uninstall the application (see Chapter 14 on p. 168).

To uninstall the application in the noninteractive mode without restarting the computer (the computer should be restarted manually after uninstalling), enter:

```
msiexec /x <package_name> /qn
```

To uninstall the application in the background and then restart the computer, enter:

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

If you opted for password protection against uninstalling the program when you installed the program, it is necessary to enter this password. Otherwise program cannot be uninstalled.

To remove the application by entering a password as evidence of the removal privilege, enter:

`msiexec /x <package_name> KLUNINSTPASSWD=******` – to remove application in interactive mode;

`msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – to remove application in non-interactive mode;

APPENDIX A. REFERENCE INFORMATION

This appendix contains reference materials on the file formats and extension masks used in Kaspersky Anti-Virus for Windows Servers settings.

A.1. List of files scanned by extension

If you select **Scan programs and documents (by extension)**, File Anti-Virus will scan files with the extensions below in-depth for viruses.

com – executable file for a program

exe – executable file or self-extracting archive

sys – system driver

prg – program text for dBase, Clipper or Microsoft Visual FoxPro, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a .bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic loading library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program that runs in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – initialization file

cla – Java class

vbs – Visual Basic script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML with built-in PHP scripts

php – script built into HTML files

wsh – Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper

hlp – Win Help file

eml – Microsoft Outlook Express email file

nws – Microsoft Outlook Express new email file

msg – Microsoft Mail email file

plg – email

mbx – extension for saved Microsoft Office Outlook emails

*doc** – a Microsoft Word document, such as: *doc* – a Microsoft Word document, *docx* – a Microsoft Word 2007 document with XML suport, *docm* – a Microsoft Word 2007 document with Macro support

*dot** – a Microsoft Word document template, such as, *dot* – a Microsoft Word document template, *dotx* – a Microsoft Word 2007 document template , *dotm* – a Microsoft Word 2007 document template with Macro support

fpm – database program, start file for Microsoft Visual FoxPro

rtf – Rich Text Format document

shs – Shell Scrap Object Handler fragment

dwg – AutoCAD blueprint database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave Flash file

jpg, jpeg, png – compressed image graphics format

emf – Enhanced Metafile format Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows

ico – icon file

ov? – *Microsoft DOC executable files*

*xl** – Microsoft Office Excel documents and files, such as: *xla* - Microsoft Office Excel extension, *xlc* - diagram, *xlt* - document templates. *xlsx* – a Microsoft Excel 2007 workbook , *xltm* – a Microsoft Excel 2007 workbook with Macro support , *xlsb* – a Microsoft Excel 2007 in binary (non-XML) format , *xltx* – a Microsoft Excel 2007 template , *xlsm* – a Microsoft Excel 2007 template with Macro support , *xlam* – a Microsoft Excel 2007 plugin with Macro support.

*pp** – Microsoft Office Excel documents and files, such as: *xla* - Microsoft Office Excel extension, *xlc* - diagram, *xlt* - document templates. *xlsx* – a Microsoft Excel 2007 workbook , *xltm* – a Microsoft Excel 2007 workbook with Macro support , *xlsb* – a Microsoft Excel 2007 in binary (non-XML) format , *xltx* – a Microsoft Excel 2007 template , *xlsm* – a Microsoft Excel 2007 template with Macro support , *xlam* – a Microsoft Excel 2007 plugin with Macro support.

*md** – Microsoft Office Access documents and files, such as: *mda* – Microsoft Office Access work group, mdb – database, etc.

sldx – a Microsoft PowerPoint 2007 slide.

sldm – a Microsoft PowerPoint 2007 slide with Macro support.

thmx – a Microsoft Office 2007 theme.

Remember that the actual format of a file may not correspond with the format indicated in the file extension.

A.2. Possible file exclusion masks

Let's look at some examples of possible masks that you can use when creating file exclusion lists:

- Masks without file paths:
  - ***.exe** – all files with the extension *.exe*
  - ***.ex?** – all files with the extension *.ex?,* where ? can represent any one character
  - **test** – all files with the name *test*
- Masks with absolute file paths:
  - **C:\dir*.*** or **C:\dir*** or **C:\dir** – all files in folder *C:\dir*
  - **C:\dir*.exe** – all files with extension .exe in folder *C:\dir*
  - **C:\dir*.ex?** – all files with extension .ex? in folder *C:\dir\,* where ? can represent any one character

- **C:\dir\test** – only the file *C:\dir\test*

- If you do not want the program to scan files in the subfolders of this folder, uncheck ☑ **Include subfolders** when creating the mask.

- Masks with relative file paths:

  - **dir*.*** or **dir*** or **dir** – all files in all *dir* folders
  - **dir\test** – all *test* files in *dir\ folders*
  - **dir*.exe** – all files with the extension *.exe* in all *dir\ folders*
  - **dir*.ex?** – all files with the extension .ex? in all *C:\dir* folders, where ? can represent any one character

  If you do not want the program to scan files in the subfolders of this folder, uncheck ☑ **Include subfolders** when creating the mask.

Tip:

. and * exclusion masks can only be used if you assign an excluded threat a verdict according to the Virus Encyclopedia. Otherwise the threat specified will not be detected in any objects. Using these masks without selecting a verdict essentially disables monitoring.

We also do not recommend that you select a virtual drive created on the basis of a file system directory using the *subst* command as an exclusion. There is no point in doing so, since during the scan, the program perceives this virtual drive as a folder and consequently scans it.

A.3. Possible Virus Encyclopedia classification exclusion masks

When adding threats with a certain status from the Virus Encyclopedia classification as exclusions, you can specify:

- the full name of the threat as given in the Virus Encyclopedia at www.viruslist.com (for example, **not-a-virus:RiskWare.RemoteAdmin.RA.311** or **Flooder.Win32.Fuxx**);

- threat name by mask. For example:

  - **not-a-virus*** – excludes potential dangerous programs from the scan, as well as joke programs.
  - ***Riskware.*** – excludes riskware from the scan.

- ***RemoteAdmin.*** – excludes all remote administration programs from the scan.

A.4. Overview of settings in *setup.ini*

The file *setup.ini*, located in the Kaspersky Anti-Virus installation folder, is used when installing the program in the noninteractive mode from the command prompt (see 3.3 on pg. 31) or using Group Policy Object Editor (see 3.4 on pg.32). The file contains the following settings :

[Setup] – general settings for program installation.

InstallDir=<path to program installation folder>.

Reboot=yes|no – whether the computer should restart after the program is installed (does not restart by default).

SelfProtection=yes|no – whether Kaspersky Anti-Virus should enable Self-Defense during installation (enabled by default).

MSExclusions=yes|no – whether exclusions that Microsoft recommends for servers should be added to the Kaspersky Anti-Virus list of exclusions.

AddPath=yes|no – whether the path to avp.com will be added to the environmental system variable %Path%.

[Components] – selects the components to install. If this group contains no items, all will be installed.

FileMonitor=yes|no – installs File Anti-Virus.

[Tasks] – enables Kaspersky Anti-Virus tasks If no tasks are specified, all tasks will run after installation. If any tasks are specified, all tasks that are not listed will be disabled.

ScanMyComputer=yes|no – task for complete scan of computer

ScanStartup=yes|no – task for scanning startup objects

ScanCritical=yes|no – task for scanning critical areas

Updater=yes|no – task for updating threat signatures and program modules

Instead of the value **yes**, you can use the values **1**, **on**, **enable**, or **enabled**, and instead of **no** you can use – **0**, **off**, **disable**, or **disabled** .

APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company’s products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company’s flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, email systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

B.1. Other Kaspersky Lab Products

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, notifications about the current status of virus activity, and fresh news. The program reads the list of available news feeds and their content from the Kaspersky Lab news server at specified intervals.

News Agent enables users to;

- See the current virus forecast .in the system tray
- Subscribe to and unsubscribe from news feeds
- Retrieve news from each selected feed at the specified interval and receive notifications about fresh news
- Review news on the selected feeds
- Review the list of feeds and their status
- Open full article text in your browser

News Agent is a stand-alone Microsoft Windows application that can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

This program is a free service provided to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. This way, users receive quick responses to questions regarding potential infectionson their computers. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky® OnLine Scanner Pro

The program is a subscription service available to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer and disinfects dangerous files. Kaspersky OnLine Scanner Pro runs directly from your browser. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks, including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used, as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, folders, or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

Controls modifications within the file system. The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.

Monitors processes in random-access memory. Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.

Monitors changes in OS registry due to internal system registry control.

Hidden Processes Monitor helps protect from malicious code concealed in the operating system using rootkit technologies.

Heuristic Analyzer. When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.

Performs system restore after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 is an integrated solution for protection of personal computers against the major information- threats (viruses, hackers, spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.

Real-time anti-virus scanning of Internet traffic transferred via HTTP.

File system protection: anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.

Proactive protection: the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks such activity. *Privacy Control* module keeps your confidential information secure from unauthorized access and transmission. *Parental Control* is a Kaspersky Internet Security component that monitors user access to the Internet.

Kaspersky Internet Security 7.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical network attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth Mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch to Stealth Mode, the system blocks all network activity except for a few transactions allowed in user-defined rules.

The program employs an all-inclusive approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites)
- Inspection of phrases in message body
- Analysis of message text using a learning algorithm
- Recognition of spam sent in image files

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile provides antivirus protection for mobile devices running Symbian OS and Microsoft Windows Mobile. The program provides comprehensive virus scanning, including:

- **On-demand scans** of the mobile device's onboard memory, memory cards, an individual folder, or a specific file; if an infected file is detected, it is moved to Quarantine or deleted
- **Real-time scanning –** all incoming and outgoing files are automatically scanned, as well as files when attempts are made to access them
- **Protection from text message spam**

Kaspersky Anti-Virus for File Servers

This software package provides reliable protection for file systems on servers running Microsoft Windows, Novell NetWare, Linux and Samba from all types of malware. The suite includes the following Kaspersky Lab applications:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Features and functionality:

- *Protects server file systems in real time*: All server files are scanned when opened or saved on the server
- *Prevents virus outbreaks*;
- *On-demand scans* of the entire file system or individual files and folders;
- *Use of optimization technologies* when scanning objects in the server file system;
- *System rollback after virus attacks*;

- *Scalability of the software package* within the scope of system resources available;
- *Monitoring of the system load balance*;
- *Creating a list of trusted processes* whose activity on the server is not subject to control by the software package;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Saving backup copies of infected and deleted objects* in case you need to restore them;
- *Quarantining suspicious objects*;
- *Send notifications on events* in program operation to the system administrator;
- *Log detailed reports*;
- *Automatically update* program databases.

Kaspersky Open Space Security

Kaspersky Open Space Security is a software package withal new approach to security for today's corporate networks of any size, providing centralized protection information systems and support for remote offices and mobile users.

The suite includes four programs:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifics on each program are given below.

Kaspersky WorkSpace Security is a program for centralized protection of workstations inside and outside of corporate networks from all of today's Internet threats (viruses, spyware, hacker attacks, and spam).

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam*;
- *Proactive Defense from new malicious programs whose signatures are not yet added to the database;*

- *Personal Firewall with intrusion detection system and network attack warnings;*
- *Rollback for malicious system modifications;*
- *Protection from phishing attacks and junk mail;*
- *Dynamic resource redistribution during complete system scans;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Scanning of e-mail and Internet traffic in real time;*
- *Blocking of popup windows and banner ads when on the Internet;*
- *Secure operation in any type of network, including Wi-Fi;*
- *Rescue disk creation tools that enable you to restore your system after a virus outbreak;*
- *An extensive reporting system on protection status;*
- *Automatic database updates;*
- *Full support for 64-bit operating systems;*
- *Optimization of program performance on laptops (Intel® Centrino® Duo technology);*
- *Remote disinfection capability (Intel® Active Management, Intel® vPro™).*

Kaspersky Business Space Security provides optimal protection of your company's information resources from today's Internet threats. Kaspersky Business Space Security protects workstations and file servers from all types of viruses, Trojans, and worms, prevents virus outbreaks, and secures information while providing instant access to network resources for users.

Features and functionality:

- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Protection of workstations and file servers from all types of Internet threats;*
- *iSwift technology to avoid rescanning files within the network;*

- *Distribution of load among server processors;*
- *Quarantining suspicious objects from workstations;*
- *Rollback for malicious system modifications;*
- *scalability of the software package within the scope of system resources available;*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database;*
- *Scanning of e-mail and Internet traffic in real time;*
- *Personal Firewall with intrusion detection system and network attack warnings;*
- *Protection while using Wi-Fi networks;*
- *Self-Defense from malicious programs;*
- *Quarantining suspicious objects;*
- *Automatic database updates.*

Kaspersky Enterprise Space Security

This program includes components for protecting linked workstations and servers from all today's Internet threats. It deletes viruses from e-mail, keeping information safe while providing secure access to network resources for users.

Features and functionality:

- *Protection of workstations and file servers from viruses, Trojans, and worms;*
- *Protection of Sendmail, Qmail, Postfix and Exim mail servers;*
- *Scanning of all e-mails on Microsoft Exchange Server, including shared folders;*
- *Processing of e-mails, databases, and other objects for Lotus Domino servers;*
- *Protection from phishing attacks and junk mail;*
- *preventing mass mailings and virus outbreaks;*

- *scalability of the software package within the scope of system resources available ;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco ® NAC (Network Admission Control);*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation while using Wi-Fi networks;*
- *Scans Internet traffic in real time;*
- *Rollback for malicious system modifications;*
- *Dynamic resource redistribution during complete system scans;*
- *Quarantining suspicious objects ;*
- *An extensive reporting system on protection system status;*
- *automatic database updates.*

Kaspersky Total Space Security

This solution monitors all inbound and outbound data streams (e-mail, Internet, and all network interactions). It includes components for protecting workstations and mobile devices, keeps information safe while providing secure access for users to the company's information resources and the Internet, and ensures secure e-mail communications.

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam on all levels of the corporate network, from workstations to Internet gateways;*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Protection of mail servers and linked servers;*
- *Scans Internet traffic (HTTP/FTP) entering the local area network in real time;*

- *scalability of the software package within the scope of system resources available ;*
- *Blocking access from infected workstations;*
- *Prevents virus outbreaks;*
- *Centralized reporting on protection status;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Support for hardware proxy servers;*
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *iSwift technology to avoid rescanning files within the network ;*
- *Dynamic resource redistribution during complete system scans;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation for users on any type of network, including Wi-Fi;*
- *Protection from phishing attacks and junk mail;*
- *Remote disinfection capability (Intel® Active Management, Intel® vPro™);*
- *Rollback for malicious system modifications;*
- *Self-Defense from malicious programs;*
- *full support for 64-bit operating systems*;
- *automatic database updates*.

Kaspersky Security for Mail Servers

This program is for protecting mail servers and linked servers from malicious programs and spam. The program includes application for protecting all standard mail servers (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim) and also enables you to configure a dedicated e-mail gateway. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.

- Kaspersky Anti-Virus for Linux Mail Server.

Its features include:

- *Reliable protection from malicious or potentially dangerous programs*;
- *Junk mail filtering*;
- *Scans incoming and outgoing e-mails and attachments*;
- *Scans all e-mails on* Microsoft Exchange Server for viruses, including shared folders;
- *Processes e-mails, databases, and other objects for Lotus Notes/Domino servers*;
- *Filters* e-mails by attachment type;
- *Quarantines* suspicious objects;
- *Easy-to-use administration system for* the program;
- *Prevents virus outbreaks*;
- *Monitors protection system status* using notifications;
- *Reporting system* for program operation;
- scalability of the software package within the scope of system resources available ;
- *automatic database updates*.

Kaspersky Security for Internet Gateways

This program provides secure access to the Internet for all an organization's employees, automatically deleting malware and riskware from the data incoming on HTTP/FTP. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Its features include:

- *Reliable protection from malicious or potentially dangerous programs*;
- *Scans Internet traffic* (HTTP/FTP) in real time;
- *Filters Internet traffic* using a trusted server list, object types, and user groups;

- *Quarantines* suspicious objects;
- *Easy-to-use administration system*;
- *Reporting system for program operation*;
- *Support for hardware proxy servers*;
- Scalability of the software package within the scope of system resources available ;
- *Automatic database updates*.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database, adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper provides high-speed scanning of traffic on servers running Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

The program is a plug-in and scans for viruses and processes inbound and outbound e-mail traffic in real time.

B.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: info@kaspersky.com

APPENDIX C. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER'S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

1. *License Grant*. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby

grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes.

1.1 *Use*. The number of computers that User may protect by the Software is specified in the License Key File and indicated in the "Service" window. The Software may not be used to protect any networks with more than this number of file servers.

1.1.1 The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab's update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.1.8 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 Removal of Potentially Harmful Products. You acknowledge and agree that, in addition to detecting harmful and malicious software, the Product may also identify, remove and/or disable potentially harmful products, including those that are regarded or classified as Adware, Riskware, Pornware etc.

2. *Support*.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of purchasing on:

  (a) payment of its then current support charge, and:

  (b) Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.

  (c) Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

(ii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iv) "Support Services" means:

  (a) Hourly updates of the anti-virus database;

  (b) Free software updates, including version upgrades;

  (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;

  (d) Virus detection and disinfection updates in 24-hours period.

(v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights*. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the

Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality*. You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavors to maintain the security of the activation code.

5. *Limited Warranty*.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Kaspersky Lab does not warrant that this Software provides protection after expiring date (see section.2 (i))

(v) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(vi) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vii) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or

purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability*.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to

this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.

When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).